Express Mail Label No. EJ803686528US

SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR PROPOSAL REPORTING USING A GRAPHICAL USER INTERFACE IN A SUPPLY CHAIN MANAGEMENT FRAMEWORK

FIELD OF THE INVENTION

The present invention relates to information storage and processing systems, and more particularly, relates to the management of supply chains using such systems.

BACKGROUND OF THE INVENTION

Many types of manufacturing database management and inventory control systems exist today. Each of these systems views the process from the narrow viewpoint of the goals of such a system. For example, inventory control processes tend to determine when the inventory of an item is projected to be depleted and when to order goods to prevent such depletion. The inventory control process does not generally take into account the problems associated with availability of materials and machines to satisfy the inventory demand. On the other hand, the manufacturing control process considers the availability problem but does not take into account the effect of a sales promotion that will deplete an inventory faster than projected. A marketing department in preparing a sales promotion will often not consider the effect that promotion will have on availability, inventory and profit margin but tends to focus on sales goals. What is needed is a system that will support managers with each of these view points in understanding the effect of the various decisions that can be made on the supply chain as a whole both currently and into the near future.

Supply chain information flows today are fragmented, limited, and, in some cases, non-existent. The lack of timely communication between the different participants in the supply chain has resulted in higher costs for the system, for example, by limiting its ability to adequately measure distributor performance or to analyze promotion and new product activities, e.g., sales success, etc. In addition, the system continues to suffer from excess inventories and waste, unnecessary stock outs and rationing of products. A company cannot effectively react to these issues because the information that is needed to make sound management decisions is not available when it is needed.

From a marketing perspective, this lack of information has significantly hampered a company's ability to evaluate marketing tactics, post-program. Such companies also do not possess historical data that can assist it in developing marketing strategy and related plans, and understanding the essence of a brand.

Today, there is limited access to, and limited participation in, supply chain information systems by restaurants, franchisees, distributors, suppliers, etc. The infrastructure for supply chain information systems is inadequate. Restaurant point-of-sale (POS) systems are diverse and do not allow for data flows and the resulting analysis. At any point in time, it is not known how much product is selling, when it is selling or where it is selling. As long as this situation is allowed to continue, activities throughout the supply chain will continue to be reactive, error-prone, time-consuming and costly.

SUMMARY OF THE INVENTION

A system, method and computer program product are disclosed for proposal reporting utilizing a supply chain graphical user interface. A proposal is identified utilizing a graphical user interface. A plurality of components of the proposal are then indicated utilizing the graphical user interface. The selection of the components is subsequently allowed utilizing the graphical user interface so that a proposal can be created utilizing the selected components.

In one aspect, the proposal may be generated utilizing templates. In another aspect, the graphical user interface may be displayed utilizing a network browser. In a further aspect, the proposal may be editable. In an additional aspect, the proposal may be read-only. In yet another aspect, the proposal may include a bid proposal for goods to be shipped from a supplier to an outlet.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure **1A** illustrates an electronic reporting and feedback system according to an embodiment of the present invention;

Figure **1B** illustrates an electronic reporting and feedback system for restaurants according to an illustrative embodiment of the present invention;

Figure **2** is a flowchart of a process for normalizing data in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **3** is a flowchart of a process for reporting in a network-based supply chain management framework in accordance with an embodiment of the present invention;

Figure **4** illustrates an infrastructure for web services according to a preferred embodiment of the present invention;

Figure **5** is a flowchart of a process for managing a supply chain utilizing a network in accordance with an embodiment of the present invention;

Figure **6** is a flowchart of a process for tracking a performance of distributors in accordance with an embodiment of the present invention;

Figure **7** is a flowchart of a process for tracking a performance of suppliers in accordance with an embodiment of the present invention;

Figure **8** is a flowchart of a process for tracking the performance of suppliers and distributors in a plurality of marketplaces in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **9** is a flowchart of a process for forecasting the sale of goods in a store utilizing a network-based supply chain management framework in accordance with an embodiment of the present invention;

Figure **10** is a flowchart of a process for inventory management utilizing a network-based framework in accordance with an embodiment of the present invention;

Figure **11** is a flowchart of a process for providing feedback on forecasting relating to the sale of goods in a store utilizing a network-based supply chain management framework in accordance with an embodiment of the present invention;

Figure **12** illustrates an integrated supply chain analysis model according to an embodiment of the present invention;

Figure **13** is a flowchart of a process for planning promotions according to one embodiment of the present invention;

Figure **14** is a flowchart of a process for assessing market trends in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **15** is a flowchart of a process for collecting data to forecast sales in a supply chain in accordance with an embodiment of the present invention;

Figure **16** is a flowchart of a process for tracking the sale of goods in a store utilizing a network-based supply chain management framework in accordance with an embodiment of the present invention;

Figure **17** is a flowchart of a process for cost reporting using a network-based supply chain management framework in accordance with an embodiment of the present invention;

Figure **18** is a flowchart of a process for forecasting the sale of goods in accordance with an embodiment of the present invention;

Figure **19** is a flowchart of a process for evaluating a success of a promotion utilizing a network-based supply chain management framework in accordance with an embodiment of the present invention;

Figure **20** illustrates levels of integration between the supply chain coordinator and retail management;

Figure **21** is a flow diagram depicting integration ownership;

Figure **22** illustrates an electronic reporting and feedback system according to a preferred embodiment of the present invention;

Figure **23** is a flowchart of a process for raw product supply chain reporting in accordance with an embodiment of the present invention;

Figure **24** is a flow diagram illustrating basic communication and product movement according to an illustrative embodiment of the present invention;

Figure **25** is a flow diagram illustrating advanced communication and product movement according to an illustrative embodiment of the present invention;

Figure **26** illustrates a Sales Forecast Worksheet presenting historical data and projected data;

Figure **27** depicts a Promotion Monitoring Worksheet illustrating statistics such as variance from expected levels;

Figure **28** is a flowchart of a process for identifying goods in a network-based supply chain management framework in accordance with an embodiment of the present invention;

Figure **29** is a flowchart of a process for generating supply chain statistics in accordance with an embodiment of the present invention;

Figure **30** depicts a sample report for a distribution center;

Figure **31** illustrates a Data Quality report;

Figure **32** illustrates a distributor ranking report;

Figure **33** depicts a sample Supplier report;

Figure **34** illustrates a Data Quality report;

Figure **35** illustrates a distributor ranking report that provides statistics on the number of orders filled, on-time deliveries, and perfect orders delivered;

Figure **36** illustrates a Food Cost Summary report that compares the actual cost of food against a projected cost;

Figure **37** is a flowchart of a process for promotion reporting in a network-based supply chain management framework in accordance with an embodiment of the present invention;

Figure **38** is a flowchart of a process for order confirmation in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **39** is a flowchart of a process for advertising in a network-based supply chain management framework in accordance with an embodiment of the present invention;

Figure **40** is a flowchart of a process for advertising in a network-based supply chain management framework in accordance with an embodiment of the present invention;

Figure **41** is a flowchart of a process for generating revenue utilizing a network-based supply chain management framework in accordance with an embodiment of the present invention;

Figure **42** is a flowchart of a process for generating revenue utilizing a network-based supply chain management framework in accordance with an embodiment of the present invention;

Figure **43A** is a flowchart of a process for an auction function utilizing a network-based supply chain management framework in accordance with an embodiment of the present invention;

Figure **43B** is a flow diagram of a process for utilizing market demand information for generating revenue;

Figure **43C** is a flow diagram of another process for generating revenue according to an embodiment of the present invention;

Figure **43D** is a flow chart of a process **4386** for risk management in a supply chain management framework;

Figure **44** illustrates an exemplary system with a plurality of components in accordance with one embodiment of the present invention;

Figure **45** is a schematic diagram of a hardware implementation of one embodiment of the present invention;

Figure **46** is a flowchart of a process for providing network-based supply chain communication between stores, distributors, suppliers, a supply chain manager, and a corporate headquarters in accordance with an embodiment of the present invention;

Figure **47** is a flow diagram of a process for providing network-based supply chain communication according to another embodiment of the present invention;

Figure **48** is a flowchart of a process for providing a restaurant supply chain management interface framework in accordance with an embodiment of the present invention;

Figure **49** is a schematic illustration of an exemplary supply chain coordinator web site start page in accordance with an embodiment of the present invention;

Figure **50** is a schematic illustration of an exemplary supply chain coordinator Members' Front Page in accordance with an embodiment of the present invention;

Figure **51** is a flowchart of a process for providing a supplier interface in accordance with an embodiment of the present invention;

Figure **52** is a flowchart of a process for providing a distributor interface in accordance with an embodiment of the present invention;

Figure **53** is a schematic illustration of an exemplary POS Implied Daily Usage – Distributor report that may be displayed in the supply chain coordinator web site in accordance with an embodiment of the present invention;

Figure **54** is a schematic illustration of an exemplary local promotion summary by distribution center report that may be displayed in the supply chain coordinator web site in accordance with an embodiment of the present invention;

Figure **55** is a schematic illustration of an exemplary POS implied daily usage - supplier report that may be displayed in the supply chain coordinator web site in accordance with an embodiment of the present invention;

Figure **56** is a schematic illustration of an exemplary retailer landed cost verification report that may be displayed in the supply chain coordinator web site in accordance with an embodiment of the present invention;

Figure **57** is a flowchart of a process for navigating a user in a network-based supply chain management interface in accordance with an embodiment of the present invention;

Figure **58** depicts a high level view of ISCM communications according to an illustrative embodiment of the present invention;

Figure **59** is a flowchart of a process for tracking the shipment of goods in a network-based supply chain management framework utilizing barcodes in accordance with an embodiment of the present invention;

Figure **60** illustrates the ISCM in the context of security and access management;

Figure **61** sets forth the members of the ISCM community and their relationship;

Figure **62** is a flowchart of a process for selecting suppliers in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **63** illustrates a multi-level, complex member organization;

Figure **64** is a flowchart of a process for contract enforcement in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **65** is a flowchart of a process for monitoring distributor activity in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **66** is a flowchart of a process for monitoring supplier activity in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **67** is a flowchart of a process for a bulletin board feature in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **68** is a flowchart of a process for a catalog feature in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **69** is an outline of an approach for mapping customers directly to solution design;

Figure **70** is a flowchart of a process for electronic invoice auditing in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **71** is a flowchart of a process for providing a network-based supply chain interface capable of maintaining the anonymity of stores in the supply chain in accordance with an embodiment of the present invention;

Figure **72** shows several applications for the web portal;

Figure **73** shows an expanded view of the portal from a security and access control perspective;

Figure **74** is a flow diagram showing how group and roles manage access;

Figure **75** is a schematic illustrating features and functions across web, network and system areas;

Figure **76** is a schematic diagram showing a validation of users on a web portal;

Figure **77** graphically shows how user roles are managed in a multi-community environment;

Figure **78** illustrates a schematic showing the protection of resources with a central policy server, a separate user directory, and the integration of affiliate sites through an agent client;

Figure **79** illustrates a policy based security architecture in accordance with one embodiment of the present invention;

Figure **80** is a flowchart of a process for a secure supply chain management framework in accordance with an embodiment of the present invention;

Figure **81** shows a schematic with attribute setting through a web interface;

Figure **82** illustrates a flow diagram for assigning default privileges;

Figure **83** shows a Zen diagram illustrating the intersection of privileges;

Figure **84** illustrates a diagram showing a system, supply chain member, retail manager, the supply chain coordinator, supplier, and distributor root nodes;

Figure **85** illustrates another diagram showing groups within domains;

Figure **86** shows still another diagram showing hierarchies in accordance with one embodiment of the present invention;

Figure **87** shows a process for hierarchy management, in accordance with one embodiment of the present invention;

Figure **88** depicts a hierarchy in the supply chain portal management, in accordance with one embodiment of the present invention;

Figure **89** illustrates the retail outlet manager as part of the supply chain coordinator hierarchy, in accordance with one embodiment of the present invention;

Figure **90** is a schematic showing the process by which cross-domain access rights are granted;

Figure **91** is a diagram that shows a process flow for an administrative function;

Figure **92** is a flowchart of a process for updating information in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **93** is a flowchart of a process for managing a health and personal care products supply chain utilizing a network in accordance with an embodiment of the present invention;

Figure **94** is a flowchart of a process for managing an electronics and appliances supply chain utilizing a network in accordance with an embodiment of the present invention;

Figure **95** is a flowchart of a process for managing a transportation equipment supply chain utilizing a network in accordance with an embodiment of the present invention;

Figure **96** is a flowchart of a process for managing a home products supply chain utilizing a network in accordance with an embodiment of the present invention;

Figure **97** is a flowchart of a process for managing a food and beverage supply chain utilizing a network in accordance with an embodiment of the present invention;

Figure **98** is a flowchart of a process for managing a machinery supply chain utilizing a network in accordance with an embodiment of the present invention;

Figure **99** is a flowchart of a process for managing an sporting good supply chain utilizing a network in accordance with an embodiment of the present invention;

Figure **100** is a flowchart of a process for managing a chemical supply chain utilizing a network in accordance with an embodiment of the present invention;

Figure **101** is a flowchart of a process for managing a department store supply chain utilizing a network in accordance with an embodiment of the present invention;

Figure **102A** is a flowchart of a process for managing an office product supply chain utilizing a network in accordance with an embodiment of the present invention;

Figure **102B** is a flow diagram of a process for managing a book supply chain utilizing a network according to one embodiment of the present invention;

Figure **103** is a flowchart of a process for managing a gas station supply chain utilizing a network in accordance with an embodiment of the present invention;

Figure **104A** is a flowchart of a process for managing a convenience store supply chain utilizing a network in accordance with an embodiment of the present invention;

Figure **104B** is a flow diagram of a process for managing a toy supply chain utilizing a network according to an embodiment of the present invention;

Figure **105** is a flowchart of a process for managing an entertainment media supply chain utilizing a network in accordance with an embodiment of the present invention;

Figure **106** is a flowchart of a process for managing an accommodation supply chain utilizing a network in accordance with an embodiment of the present invention;

Figure **107** is a flowchart of a process for a reverse auction in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **108** is a flowchart of a process for tracking damaged goods in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **109** is a flowchart of a process for allocating responsibilities in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **110** is a flowchart of a process for determining product supply parameters in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **111** is a flowchart of a process for reducing costs in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **112** is a flowchart of a process for handling contracts in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **113** is a flowchart of a process for centralizing a supply chain management framework in accordance with an embodiment of the present invention;

Figure **114** is a flowchart of a process for providing local distribution committees in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **115** is a flowchart of a process for price auditing in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **116** is a flowchart of a process for auditing performance in a supply chain framework in accordance with an embodiment of the present invention;

Figure **117** is a flowchart of a process for providing an electronic mail virtual private network in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **118** is a flowchart of a process for secret pricing in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **119** is a flowchart of a process for managing risk in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **120** is a flowchart of a process for product tracking in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **121** is a flowchart of a process for auctioning surplus products in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **122** is a flowchart of a process for managing a supply chain utilizing a network in accordance with an embodiment of the present invention;

Figure **123** is a flowchart of a process for managing a supply chain utilizing a network in accordance with an embodiment of the present invention;

Figure **124** is a flowchart of a process for disseminating calendar information in a supply chain utilizing a network in accordance with an embodiment of the present invention;

Figure **125** illustrates a graphical user interface for generating cost system components;

Figure **126** depicts a selection screen;

Figure **127** illustrates an Add Items window displayed upon selecting Items from the Supply menu and New fro the selection screen;

Figure **128** illustrates a Landed Cost Report by Distribution Center;

Figure **129** illustrates an Item/FOB button that calls up an FOB window;

Figure **130** depicts an FOB window;

Figure **131** illustrates a window for adding an FOB point;

Figure **132** depicts a screen for adding Distribution Centers;

Figure **133** is a flowchart of a process for creating cost system components in a supply chain utilizing a network in accordance with an embodiment of the present invention;

Figure **134** illustrates a matrix window for creating matrices;

Figure **135** illustrates a matrix that identifies the source and destination for a product in question;

Figure **136** illustrates an FOB matrix;

Figure **137** illustrates a contract matrix;

Figure **138** depicts a Contract button;

Figure **139** depicts a minimum order matrix;

Figure **140** illustrates a shipping matrix;

Figure **141** shows an Options menu;

Figure **142** illustrates a Notification toolbar button;

Figure **143** illustrates selection of a Multi-Item Price Notification;

Figure **144** is a flowchart of a process for utilizing cost models in a supply chain utilizing a network in accordance with an embodiment of the present invention;

Figure **145** depicts a New Item button;

Figure **146** illustrates a Contract/Buyer association screen;

Figure **147** depicts a contract schedule screen;

Figure **148** illustrates a Generate button;

Figure **149** illustrates an Exhibit A button, which upon selection provides the Supplier with the "Approved Products" listing for the current contract;

Figure **150** illustrates an Exhibit B button, which upon selection provides the detail on per case pricing and volume for each lane assigned to this Supplier;

Figure **151** shows a screen for selecting end dates to use on an exhibit;

Figure **152** illustrates an Options drop down menu;

Figure **153** depicts an Exhibit C button for generating a report which lists product routing for each lane and any minimum order quantities;

Figure **154** is a flowchart of a process for creating a contract utilizing a supply chain graphical user interface in accordance with an embodiment of the present invention;

Figure **155** shows a Proposal submenu;

Figure **156** illustrates a Bid Proposal window used for generating a proposal;

Figure **157** illustrates toolbar buttons for adding, deleting and printing actions;

Figure **158** illustrates a page under the Items tab;

Figure **159** illustrates the page under the Items tab upon selection of the Search button;

Figure **160** illustrates a page under the FOB Price tab for selecting FOB price component worksheets;

Figure **161** depicts a window for managing Distribution Center usage;

Figure **162** is a flowchart of a process for creating a bid proposal utilizing a supply chain graphical user interface in accordance with an embodiment of the present invention;

Figure **163** illustrates a Templates button which calls a Template window;

Figure **164** depicts the Template window called by the Templates button;

Figure **165** illustrates a window displayed upon selection of the Templates tab;

Figure **166** is an illustration of a Microsoft Word menu;

Figure **167** is an illustration of the page presented upon selection of the Create Bid tab;

Figure **168** shows a Create Bid button;

Figure **169** illustrates a drop down list box from which a user can select reports for viewing;

Figure **170** illustrates a Print button;

Figure **171** depicts a Print Bid button;

Figure **172** is a flowchart of a process for proposal reporting utilizing a supply chain graphical user interface in accordance with an embodiment of the present invention;

Figure **173** depicts a Least Cost toolbar button;

Figure **174** illustrates a standard query screen;

Figure **175** shows a Supply menu;

Figure **176** depicts a drop down list for changing Bid selection;

Figure **177** is a flowchart of a process for analysis creation utilizing a supply chain graphical user interface in accordance with an embodiment of the present invention;

Figure **178** illustrates a window displayed upon beginning an analysis;

Figure **179** depicts an option selection window;

Figure **180** illustrates a version button for creating new versions of analyses;

Figure **181** illustrates a verification window that appears upon selection of the version button;

Figure **182** is a flowchart of a process for analysis version control in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **183** depicts a tab page for adding and removing FOBs from an analysis;

Figure **184** illustrates a portion of the Item tab page;

Figure **185** is a flowchart of a process for editing supplier information in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **186** illustrates a page that is displayed upon selection of the Item/FOB tab;

Figure **187** shows an Update button for updating cost information;

Figure **188** is a flowchart of a process for adding components in a supply chain management analysis in accordance with an embodiment of the present invention;

Figure **189** is an illustration of an exemplary analysis window displayed upon selecting a Capacity tab;

Figure **190** illustrates another analysis window;

Figure **191** is a flowchart of a process for managing supplier sites in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **192** is a depiction of an FOB pricing window;

Figure **193** depicts an illustrative FOB Volume Pricing screen;

Figure **194** depicts a Supplier Volume Pricing window;

Figure **195** shows a Delivered Pricing screen;

Figure **196** is a flowchart of a process for pricing in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **197** is a depiction of a Projected Restaurant Growth screen;

Figure **198** illustrates a Projected Usage Estimation screen;

Figure **199** is a flowchart of a process for projecting distribution center usage in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **200** illustrates an Excluding Lanes screen displayed upon selection of a Lane Restrict tab;

Figure **201** is a depiction of a Forcing Lanes window;

Figure **202** depicts a message screen;

Figure **203** is a flowchart of a process for restricting lanes in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **204** is an illustration of a Truckload Freight window displayed upon selection of a TL Freight tab;

Figure **205** illustrates an LTL Freight page;

Figure **206** is a flowchart of a process for managing freight in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **207** depicts a restriction window;

Figure **208** is a flowchart of a process for imposing regional restrictions in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **209** shows a Routing button;

Figure **210** illustrates a Report Selection window;

Figure **211** is a flowchart of a process for product routing in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **212** illustrates a Solve button;

Figure **213** illustrates the Report Selection window which allows selection of the report type;

Figure **214** illustrates a Report Name drop down list of related reports;

Figure **215** illustrates another Report Name drop down list of related reports;

Figure **216** shows a Report Selection window;

Figure **217** depicts a report name drop down list;

Figure **218** illustrates parameter entry fields for report generation;

Figure **219** shows a Retrieve button for retrieving a report;

Figure **220** is a flowchart of a process for comparison reporting in a supply chain management framework in accordance with an embodiment of the present invention;

Figure **221** illustrates a Cost button;

Figure **222** is a depiction of a Cost Matrix Creation window;

Figure **223** illustrates the Formula Pricing submenu of the Supply drop down menu;

Figure **224** illustrates a Formula Pricing window;

Figure **225** depicts the page displayed upon selecting the Pricing Tab;

Figure **226** shows a message window;

Figure **227** is an illustration of another message window;

Figure **228** depicts a selection window to allow selection of the pricing data that the user wants to copy over the current pricing;

Figure **229** is an illustration of the page displayed upon selection of the Freight Tab;

Figure **230** is a depiction of the page displayed upon selection of the Formulas Tab;

Figure **231** illustrates the page displayed upon selection of the Block Cost Tab;

Figure **232** is a depiction of the page displayed upon selection of the Adjustments Tab;

Figure **233** depicts toolbar icons used to insert or delete adjustments;

Figure **234** illustrates an RM Letter icon;

Figure **235** illustrates the Formula Maintenance window that is used to modify or add new formulas; and

Figure **236** illustrates a Formula Pricing submenu from which a user can open the Formula Maintenance window.

DETAILED DESCRIPTION

The present invention allows participants in a supply chain for an enterprise or collection of enterprises to function as an integrated system. The Supply Chain model of the present invention is responsive and efficient, based on electronic access to critical information that is available when it is needed at various points throughout the Supply Chain. As a result the Supply Chain is highly flexible, reliable and user friendly, responsive to consumer demands, able to respond to short lead times and able to significantly lower Supply Chain costs.

The present invention positions a Brand for growth, competition and profitability by installing and managing the infrastructure that facilitates accurate, timely and relevant information flows throughout the Supply Chain.

The present invention overcomes traditional difficulties with supply chain information flows, namely that the flow of information is fragmented, untimely, and/or nonexistent. Further, the present invention overcomes deficiencies in prior art supply chain information systems such as limited access; limited participation; and inadequate infrastructure; which result in the unavailability of accurate, timely management information from Supply Chain activities; business decisions not being based on the best information; unfavorable impact on the cost of products; and error prone, time consuming, and costly activities throughout the Supply Chain.

The organizational structure, technology applications and information systems that form portions of the Supply Chain are enablers that allow for effective management of the Supply Chain. The methodology of the present invention provides the means to efficiently capture, analyze and feed back timely Supply Chain data to the appropriate parties.

The claimed invention is applicable to many different industries, including but not limited to, pharmaceuticals, health and personal care products, computer and internet

technology, automotive, home product supply, food and beverage, telecommunications, machinery, air conditioning and refrigeration, chemical, department store supply, office product supply, aircraft and airline related industries, education, consumer electronics, hotel, gasoline stations, convenience stores, music and video, etc. For purposes of illustration only, portions of the following description will be placed in the context of a Supply Chain for food services, including food distribution, retail outlet management and operation, and marketing. One skilled in the art will appreciate that the various embodiments and concepts of the present invention are applicable to a plethora of industries without straying from the spirit of the present invention. As such, the scope of the present invention is to be in no way limited to food services only.

Overview

The present invention includes a supply chain management system involving at least one supply chain participant. Supply chain participants include a supply chain manager. The supply chain manager may be a supply chain participant, a department of, division of or consultant for a supply chain participant, or an independent entity unrelated to the other supply chain participants. The supply chain manager may be allowed to exercise management rights without taking title or possession of any goods passing through the supply chain.

Supply chain participants may also include brand owners, point of sale outlets, point of sale outlet owners, a cooperative or consortium of point of sale outlet owners, distributors, or suppliers. Suppliers may supply one or more of finished goods, partially finished goods or raw materials.

The supply chain management system of the present invention includes six system components which may be integrated independently, on a parallel path, but ultimately are able to electronically interface with each other. Typically, a supply chain may include retailers, distributors and suppliers or equivalents thereof.

The supply chain management system according to one aspect of the present invention, increases the Quality Of Service (QOS) to supply chain participants, lowers costs and adds new value to supply chain participants with its "predictive" nature based on statistically driven models, discussed below.

Supply chain participants, as used herein, refers without limitation to stores and other vendors/outlets, distributors, suppliers, etc. Further, suppliers include suppliers of raw, partially finished, and finished goods.

In general, the supply chain management system integrates various components, which components may include:

1. In-Retailer Systems
2. Retailer/Distributor Electronic Interface
3. Supplier/Distributor Electronic Interface
4. Data Warehouse
5. Information Services
6. Web Architecture and Internet Access

It should be understood that some or all of these components or analogous components may also be applicable to various industries including those industries set forth above.

Figure **1A** illustrates an electronic reporting and feedback system **100** according to an embodiment of the present invention.

In-Retailer Systems support point of sale outlet owners **102** with Point of Sale (POS) and BOH hardware and software solutions, and provide leadership in the evolution of retailer systems to ensure electronic connectivity to the Supply Chain. This component enables electronic data collection of daily menu item sales for the information database. It also enhances retailer operations by providing retail outlet managers with tools that help free their time to focus on the customers.

Retailer-Distributor Electronic Interface establishes an electronic purchasing system and thus "electronic commerce" between POS outlets **104** and distributors /"direct" suppliers **106,108**. This includes electronic order entry (via Web or BOH), order confirmation, product delivery/receiving, electronic invoicing, electronic wire payment transfers, data collection, and most important, contract compliance and distributor performance measurement, which assists in managing distributor performance.

Supplier-Distributor Electronic Interface facilitates the development of electronic commerce between system suppliers and distributors including electronic ordering and confirmations, electronic invoicing and payments and electronic supplier performance measuring and reporting. Electronic commerce between raw material suppliers **110** and suppliers is also provided.

Data Warehouse **112** is a central collection point that electronically collects and warehouses timely, critical Supply Chain information for all Supply Chain participants. This includes distributor and supplier performance measures, representations of daily outlet item sales with translations to specified product requirements, and inventory levels, sales history and forecasts at various points in the Supply Chain, thereby providing a basis for collaborative planning and forecasting. The data stored in the Warehouse is then available for quick, secure access.

Information Services analyzes **114**, organizes and feeds back Supply Chain data to meet the information needs of Supply Chain end users such as a brand owner **116**, the Supply Chain Coordinator (SCC) **118**,retail outlet management **120**. This includes information on Supply Chain performance, collaborative planning and forecasting, promotion planning and inventory management. Services that benefit franchisees include electronic invoice auditing, distributor performance reporting, food cost reporting and analysis, franchisee sales/cost comparables, and other reports. Information Services also determines a proper format in which to present the data so that it is in the most useful

form for the end user. It also works with Supply Chain users to develop/evaluate analytical/operational tools.

Web Architecture **122**—underlying all this electronic activity is technology, the web architecture with Internet access (through proprietary service or an Internet Service Provider (ISP)) that allows these electronic communications to take place efficiently and effectively. Encompassed in this component is the building of initial web applications and security for the Supply Chain.

Figure **1B** illustrates the electronic reporting and feedback system **100** of Figure **1A** adapted for restaurants according to an illustrative embodiment of the present invention. In this situation, the POS outlet comprises a restaurant **126**, a franchisee **124** is the POS outlet owner, and end users include restaurant management **128** and other end users **130**.

Figure **2** is a flowchart of a process **230** for normalizing data in a supply chain management framework. A plurality of data types are defined with each data type including parameters in operation **232**. Data is received utilizing a network from a plurality of POS outlets of a supply chain that relates to an amount of goods sold by the POS outlets in operation **234**. A format of the data is verified against the parameters of the defined data types in operation **236** and any discrepancies between the format of the data and the parameters of the defined data types are corrected for facilitating an analysis of the data in operation **238**.

In one aspect, the corrections may be logged. In another aspect, the discrepancies may be displayed utilizing a network-based interface. In a further aspect, discrepancies may be corrected by translating the format of the data in accordance with the parameters of the defined data types. In another aspect, the network may include the Internet. In an additional aspect, the corrected data may be displayed utilizing a network-based interface.

Figure **3** is a flowchart of a process **330** for reporting in a network-based supply chain management framework. Utilizing a network, data is received from a plurality of stores, distributors and suppliers of a supply chain in operation **332**. The data is processed in operation **334**. Subsequently, a request is received from a user for the processed data in operation **336**. The user is then identified as either relating to a store, distributor or supplier in operation **338** and the processed data is formatted based on the identification of the user as a store, distributor or supplier in operation **340**.

In one aspect, the format may includes a first format for the store, a second format for the distributor, and a third format for the supplier. In another aspect, the format may utilize a coding scheme unique to the user. In an additional aspect, the formatted, processed data may be made accessible via a network-based interface. In a further aspect, the network may include the Internet. In yet another aspect, the request may be received utilizing the network.

Figure **4** illustrates an infrastructure **400** for web services according to a preferred embodiment of the present invention. As shown, application services **402** are at the core of the infrastructure. Secondary components include hosting services **404**, content delivery **406**, and network services **408**. Professional services **410** are provided for each of the components. Additional services can include support for electronic commerce, eMarketing, eSales, and eFulfillment.

Figure **5** is a flowchart of a process **530** for managing a supply chain utilizing a network. Data is received from a plurality of restaurants of a supply chain utilizing a network in operation **532**. This data relates to the sale of goods by the restaurants. An electronic order form for ordering a plurality of goods is then generated based on the data in operation **534**. The electronic order form is subsequently transmitted to at least one supply chain participant utilizing the network in operation **536**. For example, the form can be transmitted to a distributor of the supply chain utilizing the network via a restaurant-distributor interface. The electronic order form can also be transmitted to at least one supplier of the supply chain utilizing the network via a distributor-supplier

interface. Information relating to at least one of the operations in the above process for managing the supply chain is tracked by the restaurant in operation **538**.

In one aspect, the data may be transmitted to the supply chain participants. In such an aspect, the data may be parsed to match each corresponding supply chain participant. The data may also be made accessible to the supply chain participant via a network-based interface. In another aspect, the data may be accessible to the supply chain participant only after verification of an identity of the supply chain participant. In an additional aspect, the tracked information may relate to each of said operations of the above process.

Figure **6** is a flowchart of a process **630** for tracking a performance of distributors in which a plurality of distributors are registered in operation **632**. Data is received utilizing a network in operation **634**. This data relates to the distribution of goods to a plurality of stores by the registered distributors. A performance of the registered distributors is then tracked utilizing the data in operation **636**.

In one aspect, the data may include delivery dates associated with the goods. In such an aspect, the performance may be tracked by comparing the delivery dates with a plurality of target dates. As another aspect, the performance may be tracked by comparing the delivery dates with delivery dates associated with other distributors. In another aspect, the performance may be displayed to the stores utilizing a network-based interface. In a further aspect, the data relating to the distribution of goods may be received from the stores.

Figure **7** is a flowchart of a process **730** for tracking a performance of suppliers. In general, a plurality of suppliers are registered in operation **732**. Data is then received utilizing a network in operation **734**. This data relates to the supply of goods to a plurality of distributors by the registered suppliers. A performance of the registered suppliers is tracked utilizing the data in operation **736**.

In an aspect, the data may includes inventory levels associated with the goods. As an aspect, the performance may be tracked by comparing the inventory levels with a plurality of target inventory levels. As another aspect, the performance may be tracked by comparing the inventory levels with inventory levels associated with other suppliers. In another aspect, the performance may be displayed to the stores utilizing a network-based interface. In a further aspect, the data may be received from the stores.

Figure **8** is a flowchart of a process **830** for tracking the performance of suppliers and distributors in a plurality of marketplaces in a supply chain management framework. In operation **832**, a plurality of distributors and suppliers are registered each in one of a plurality of marketplaces with each marketplace involving the supply and distribution of at least one of a plurality of goods used by a plurality of stores. Data is received utilizing a network that relates to the distribution and supply of goods to the stores by the registered distributors and suppliers in each of the marketplaces in operation **834**. The received data is parsed based on marketplaces in operation **836** and a performance of the registered distributors and suppliers is tracked in each of the marketplaces utilizing the data in operation **838**.

In one aspect, the data includes delivery dates associated with the goods. In such an aspect, the performance may be tracked by comparing the delivery dates with a plurality of target dates. As another aspect, the performance may be tracked by comparing the delivery dates with delivery dates associated with other distributors. In another aspect, the performance is displayed to the stores utilizing a network-based interface. In a further aspect, the data includes inventory levels associated with the goods. In such an aspect, the performance may be tracked by comparing the inventory levels with a plurality of target inventory levels. As another aspect, the performance may be tracked by comparing the inventory levels with inventory levels associated with other suppliers.

Results

The present invention makes critical performance information available to the Supply Chain system. The timeliness and level of detail of this information enable the supply chain coordinator to manage distributors and suppliers at standards prior art systems have been unable to achieve before. For example, timely performance information is provided against which Supply Chain management (coordinator) can take immediate action. Such performance information includes system inventory levels and movement, ordering activity, order fill rates, on-time deliveries, and product quality issues. Note that the supply chain coordinator may or may not hold an ownership interest in the other supply chain participants. Further, the supply chain coordinator does not need to be associated with the other participants in any way other than in relation to supply chain management.

Significant opportunities exist for Supply Chain participants to realize substantial savings and marketing opportunities through improved speed to market for promotions and more responsive inventory management.

Further, retailer management is given online access to the full Supply Chain database, subject to maintaining the confidentiality of individual franchisees/ retailers. For the very first time, retail outlet management will be able to evaluate Supply Chain and retail outlet sales information to develop Brand menu and marketing program strategies. In addition, another first, retailer management is allowed to evaluate the success of past marketing programs by comparing actual sales to forecasts and reviewing Gross Profit Margin analyses of programs.

According to an embodiment of the present invention, Supply Chain management is able to provide online local promotion information to distribution centers, suppliers, Field Marketing, ADIs and Local Distribution Committees. This improves the speed to market for promotions and new products, as well as provides the ability to make ongoing program adjustments.

The advantages of being able to share and update a common data base at the convenience of all users provides enhanced coordination between all participants, improved planning,

less over-ordering and product waste, and less time spent managing and coordinating local promotions. For new contracted distributors, daily distributor invoice feeds can be established.

Franchisees are provided with many advantages. Tools are provided to evaluate and select new retail POS and BOH hardware and software systems for system-wide communication with their retailers, each other and with the Supply Chain. They are given the ability to order products and manage inventory electronically, and are given access to valuable management information and tools.

Retailers are provided with the ability to conduct efficient electronic commerce with distributors and "direct" suppliers. They are also allowed to communicate easily with the Supply Chain.

Business Analysis

Figure **9** is a flowchart of a process **930** for forecasting the sale of goods in a store utilizing a network-based supply chain management framework. Data relating to a supply chain is collected in operation **932**. The selection of one or more of a plurality of points in the supply chain is also allowed in operation **934** so that the data for the selected point in the supply chain may be analyzed in operation **936**. Based on this analysis, a forecast is made of one or more aspects of the supply chain at the selected point in the supply chain in operation **938**.

In one aspect, one of the points may be a store. In such an aspect, the data may reflect a sale of goods in the store. In another aspect, one of the points may be a supplier. In further aspect, one of the points may be a distributor. In an additional aspect, the forecast may be displayed utilizing a network-based interface.

Figure **10** is a flowchart of a process **1030** for inventory management utilizing a network-based framework. Data is received from a plurality of stores of a supply chain utilizing a

network in operation **1032**. This data relates to an amount of goods sold by the stores. A recipe associated with each of the goods is identified in operation **1034** and information on processed products required to produce the goods is then calculated based on the data and the recipe in operation **1036**. The information on the processed products is outputted utilizing the network for managing the supply chain in operation **1038**.

In one aspect, the data may include an amount of the goods, and can be based on a function of menu demand. In another aspect, the recipe may indicate a type and an amount of the processed products required to produce each of the goods. In an additional aspect, the information may indicate a type and an amount of the processed products. For example, the demand for beef can be calculated. In a further aspect, the information may be outputted utilizing a network-based interface. In yet another aspect, the network may include the Internet.

Back orders can be reconstructed. Also, key demand information is gathered directly from the store, greatly increasing accuracy and reducing response time.

Sales forecasting and inventory management are components in an embodiment of the Supply Chain management system. A theme of this model is transparent communication of current (i.e. virtually real-time) and expected sales to some or all supply chain participants in a statistically meaningful distribution everyday for all inventory level products. In other words, predictive supply chain behavior can be determined and analyzed. Of course the counterbalance here is the commitment to maintain the confidentiality of the particular data source/franchisee.

Sales forecasting and analysis includes the accurate forecasting of menu items sales, monitoring system performance against forecasts, and communicating critical information to customers.

The sales forecasting and reporting subsystem allows Supply Chain management to develop, maintain and communicate sales forecasts to supply chain constituents

including, for example: 1) the franchisee community; 2) the distribution community; and 3) the supplier/manufacturing community. Some benefits of this activity include: 1) optimization of inventory levels throughout the supply chain; 2) improved logistics management; 3) improved production planning; and 4) improved promotion planning, including promotion marketing and execution. Further benefits include reduction in obsolete inventory cost, reduction in lost sales due to shortages, improved promotional decision making, reduction in supply chain cost through improved inventory and capacity management, and improved invoice averaging and revenue planning and reconciliation.

One aspect of the present invention provides an analytic model which enables a large and extended ecosystem, comprised of many similar but otherwise independent operating units, to quickly and inexpensively share near-real time data, with a trusted 3rd party, from a selected (and non-disclosed) sources, in a highly granular format, and then have extracted meaningful projections of future behavior for all of the other independent operating units so as to effect their purchase decisions. The combination of (a) confidential and very specific data, (b) accumulated quickly and cheaply, (c) shared to similar operating units, (d) leading to predictive supply chain decisions for the benefit of manufactures, suppliers, distributors and operators is a major benefit provided by the present invention.

Figure **11** is a flowchart of a process **1130** for providing feedback on forecasting relating to the sale of goods in a store utilizing a network-based supply chain management framework. Forecasting of at least one aspect of a supply chain is performed in operation **1132** based on a first set of data collected from a plurality of stores of the supply chain utilizing a network. The first set of data relates to an amount of goods sold by the stores. A second set of real-time data is collected from the stores utilizing the network in operation **1134**. The second set of real-time data relates to the amount of goods sold by the stores. The second set of real-time data is compared against the forecasting in operation **1136** and the results of the comparison are fed back for facilitating supply chain management in operation **1138**.

In an aspect, the results of the comparison are fed back utilizing a network-based interface. In another aspect, the results of the comparison include a percent difference between the first set of data and the second set of data. In a further aspect, the network includes the Internet. In one embodiment, the aspect of the supply chain includes sales of goods. In another embodiment, the aspect of the supply chain includes a demand of raw products required to produce the goods.

Overall Business Analysis Model

The sales forecasting and inventory management model is best described in the larger context of an integrated supply chain analysis model **1200**, shown in Figure **12**. This is done to reflect the fact that there are multiple customers of this information with different requirements. Sales forecasting and inventory management can be viewed as separate but interdependent analytic activities due to the core competencies, information, and systems that are required to support each.

As shown in Figure **12**, data such as menu item sales is collected in a database **1202**. An integrity check can be performed prior to storing the data in a database. Various types of analysis are performed on the data and reports are generated by Report Management **1204** and are sent to participants in the Supply Chain, who may then distribute them to external customers. The analysis and reporting processes are described in more detail below.

Sales Forecasting and Inventory Management Process

Figure **13** is a flowchart of a process **1330** for planning promotions in which historical data is collected utilizing a network from a plurality of stores of a supply chain in operation **1332**. This historical data relates to at least the sale of goods by the stores and can be further categorized based on seasonality, past marketing and/or advertising support, etc. A promotion is then planned based on the historical data in operation **1334**

and this planning is subsequently communicated to the stores utilizing the network in operation **1336**.

In one aspect, the planning may be communicated utilizing a network-based interface. In another aspect, the network may include the Internet. In a further aspect, the promotion may be planned by coinciding a time frame of the promotion with a time frame reflected by the historical data. As a further aspect, the promotion may be planned by coinciding a start time of the promotion with a start time reflected by the historical data. In an additional aspect, the promotion may be planned by selecting an amount of ordered goods of the promotion based on an amount of ordered goods reflected by the historical data. In even another aspect, an impact of the promotion on a promotional item may be forecasted. Additionally, the impact of the promotion on a non-promotional item may also be forecasted.

Figure **14** is a flowchart of a process **1430** for assessing market trends in a supply chain management framework. A network is utilized in operation **1432** to receive data that relates to the sale of goods by a plurality of stores in a plurality of regions. The received data is tagged with a date on which it was collected in operation **1434** and then organized by region and dates in operation **1436**. Market trends are then assessed utilizing the organized data in operation **1438**.

In one aspect, the network includes the Internet. In another aspect, the market trends are assessed via a network-based interface. In a further aspect, the market trends are assessed utilizing a graph. As a further aspect, the graph may include dates as one coordinate.

Figure **15** is a flowchart of a process **1530** for collecting data to forecast sales in a supply chain. Utilizing a network in operation **1532**, data is received from a plurality of stores of a supply chain that relates to an amount of goods sold by the stores. Information is also collected in operation **1534** that relates to a plurality of variables such as weather, competitor activity, and/or a marketing calendar – which may include one or more of the following types of information: cyclical sales, seasonality, historical performance of same

or similar products, and elements of marketing support. The data is processed based on the information relating to the variables in operation **1536** and a forecast of sales is generated based on the processing in operation **1538**.

In one aspect, the all of the variables (weather, competitor activity, and marketing calendar) are utilized. In another aspect, the information relating to the weather includes weather forecast. In a further aspect, the information relating to the competitor activity includes a forecast of a promotion of a competitor. In an additional aspect, the information relating to the marketing calendar includes a forecast of a promotion of the stores. In one aspect, the network includes the Internet.

As part of the data needs analysis, there are three different processes that address the issue of improving supply chain performance during promotional periods. These processes are:

Zero tolerance - meaning that there was no tolerance for either excess inventories after the promotion, nor is it appropriate to run out of product during the promotion.

While supplies last - meaning that the promotion was active until each all of the product was depleted.

Estimated Usage Report (EUR) - this is similar to the current FOR process that is used for premiums purchasing.

One objective of the sales forecasting and reporting system is to provide timely information to the supply chain allowing for: production, inventory and logistics planning; reaction to deviations from plan as quickly as possible; and/or volume estimates in support of contracting processes.

According to an illustrative embodiment of the present invention, a sales forecasting methodology is based on weekly menu item sales information. These sales forecast are

all promotion centric, which is appropriate for this example, given that many businesses run promotions several weeks per year. The process begins with an analyst extracting appropriate comparative sales data based on the type of promotion. This data is formatted in a manner that allows analyst to observe the following data:

- National Promotion Description
- Advertising Commitment in GRPs
- Premium Promotion
- Premium Advertising Commitment in GRPs
- Date of Promotion
- Average Weekly Sales Volume during Promotion Period
- Average Daily Sales of Key Menu Items During Promotion

Based on this information, the analyst makes a best guess of sales increases and cannibalization impacts. This menu item sales forecast is then translated into product requirements at the distributor and manufacturer/supplier level and communicated to the system.

A preferred sales forecasting and reporting system provides weekly forecasts for management of product volumes during promotion periods. The forecast horizon in this example is 3-6 months and can be in terms of average weekly menu item sales, with a particular focus on promotions and cannibalization.

In a food service supply chain, for example, historical menu item sales information is available by restaurant by day for geographically distributed restaurants. Exogenous variables should include: promotion type, GRP's for promotion, any other concurrent promotional activities, seasonality, competitive environment, and other factors that can be identified.

Figure **16** is a flowchart of a process **1630** for tracking the sale of goods in a store utilizing a network-based supply chain management framework. Data is received from a

plurality of stores of a supply chain utilizing a network in operation **1632**. This data relates to the sale of goods by the stores and is in a first format associated with the stores. This data is then sent from the stores to a supply chain manager (also known as a supply chain coordinator) utilizing the network in operation **1634** where the data is translated into a second format associated with the supply chain manager in operation **1636**.

In an aspect, the stores may include restaurants. In such an aspect, the data in the first format may include daily totals. These daily totals may reflect a price associated with the goods. As a further aspect, the data in the second format may include monthly totals. As another aspect, the data in the second format may include a grouping of the goods.

Preferably, data collection and reporting is in a format that allows for derivation of product requirements to support forecasted menu item sales (i.e. how many boxes of hamburger patties are required based on menu item sales forecast). Actual sales are tracked against forecasted sales on a daily basis and alerts are generated if the deviation is significant. Sales forecasting accuracy reports and post promotion analysis are provided. The sales forecast can be in a form that allows for gross profit analysis to be developed.

Some benefits to retailer outlets from the collection and analysis of information include feedback of comparative and operation information including sales mix trends, actual and/or standard (or ideal) product cost, actual and/or standard (or ideal) gross margin, and comparable information from participating retailers on this information.
Supply chain providers benefit by having access "real- time" sales information. This drives efficiencies in two ways: 1) Management of promotional volumes and inventories, and 2) Management of on going production planning. Regarding promotional volumes and inventories, supply chain providers are permitted to react faster by having sales information up to many weeks earlier than currently available. With respect to production planning, by having "real-time" sales information, suppliers are able to maintain lower safety stocks, improving capital efficiency.

Many of the benefits from "Integrated Supply Chain Management" are derived from the ability to deliver useful information for planning and operational purposes. The coordinator of the supply chain is given the information required to further optimize and decrease supply chain costs, especially for promotion management and risk management.

Figure **17** is a flowchart of a process **1730** for cost reporting using a network-based supply chain management framework. Data is received utilizing a network in operation **1732**. This data relates to goods required by a plurality of stores including a product identifier parameter, and a first cost parameter. A second cost parameter associated with a franchise mark-up is also received in operation **1734** so that a total cost can be calculated based on the first cost parameter and the second cost parameter in operation **1736**. The total cost is displayed utilizing the network with TCP/IP protocol in operation **1738**.

In an aspect, the total cost may be calculated by adding the first cost parameter and the second cost parameter. In another aspect, the total cost may be displayed utilizing a network-based interface. In a further aspect, the data may be received from a plurality of distributors. In such an aspect, the data may relate to goods required by a plurality of stores from the distributor. In one aspect, the network may include a wide area network. The sales and forecasting system can also provide longer-term forecasts, which supports contracting processes. The forecast horizon is variable based on contract needs, such as 1-5 years. The forecast can be in terms of retailer average weekly item sales. System level forecasts can be extrapolated from average weekly item sales forecasts. Historical item sales information is made available by retailer by day. Some exogenous variables include: store count, comparable sales changes, and changes in sales mix.

Preferably, data collection and reporting is in a format that allows for derivation of product requirements to support forecasted item sales. Forecasts and reports can be distributed via the Internet in a fixed report format or Excel spreadsheet, for example, depending on the recipient of the information.

Figure **18** is a flowchart of a process **1830** for forecasting the sale of goods. Data is received in operation **1832** utilizing a network from a plurality of point of sale outlets (e.g., retailers) of a supply chain where the data relates to an amount of goods sold by the point of sale outlets. The data is checked for errors in operation **1834**. Each detected error is identified in operation **1836** as either a point of sale set-up error, a point of sale entry error, a back office error, a polling error, or a menu item mapping error so that the data can be corrected using the identification in operation **1838**.

In an aspect, the network may include the Internet. In another aspect, the data may be checked for errors in real-time. In a further aspect, the identified errors may be logged. As an aspect, the log may be transmitted to the point of sale outlets utilizing the network. As another aspect, the log may be transmitted to a supply chain manager utilizing the network.

Figure **19** is a flowchart of a process **1930** for evaluating a success of a promotion utilizing a network-based supply chain management framework. Data from a plurality of stores of a supply chain is received utilizing a network in operation **1932**. This data relates to the sale of goods by the stores. A time frame of a plurality of past promotions is identified in operation **1934** and the data for each of the past promotions is analyzed utilizing the associated time frame in operation **1936**. The resulting analyses of the past promotions are then compared in operation **1938**.

In an aspect, the stores may include restaurants. In another aspect, the past promotions may then be ranked. In a further aspect, the comparison may be displayed utilizing a network-based interface. In one aspect, the time frame may include a start date and a finish date. In an additional aspect, the data may include an amount of revenue associated with the sale of the goods.

To accomplish the forecasting and reporting objectives of the present invention, some integration may be required between the supply chain coordinator and retail management. Figure **20** illustrates potential levels of integration between the supply chain coordinator

2000 and retail management 2002. At the highest level, the two are autonomous. The two may share their own forecasts, or may collaborate to create forecasts. The ideal situation is one in which a separate business unit is supported by the two. This leverages resources, eliminates bias, joins forecasts and implications of results, and provides for sharing of knowledge.

Figure 21 is a flow diagram depicting integration ownership. As shown, data flows from business process and data collection points 2102 to integration points 2104. The definition of the integration point parameters are owned by the owners of the business process and data collection point of the same border style.

Data Collection

Figure 22 illustrates an electronic reporting and feedback system 2200 according to a preferred embodiment of the present invention. As shown, data is received several of the participants in the Supply Chain and stored. Reports are generated and sent back to some or all of the participants. Also note that retail management 2202 and the supply chain coordinator 2204 are also allowed to perform their own analyses and provide feedback to other members of the Supply Chain.

Collection of Menu Item Sales

The primary element of forecasting is the communication of product movement throughout the system. Sales information can be received from suppliers and distribution centers monthly, weekly, daily, etc. Preferably, sales data from the POS by store is received daily, as it provides much more information regarding specific menu items and promotional items.

The collection and dissemination of this data allow both the supply chain coordinator and the franchisee to benefit by sharing sales information and sales forecasting. The system also benefits from improved supply chain performance. Further benefits include

providing franchisees with access to new reports on sales mix, food cost and distributor performance; and providing franchisees with a better understanding of menu sales mix on margins both in everyday situations as well as promotional situations. The supply chain coordinator, suppliers and distributors have access to virtually real-time sales, allowing for improved management of inventory and improved sales forecasting. Margin management information improves the supply chain coordinator's decision making capability in the area of risk management and purchasing.

Figure **23** is a flowchart of a process **2330** for processed product supply chain reporting wherein a network is utilized to receive data from a plurality of stores of a supply chain in operation **2332**. The data includes a first set of information relating to an amount of processed product distributed to the stores and a second set of information relating to the sale of finished product by the stores. The network is also utilized to send the data from the stores to a supply chain manager in operation **2334** where a percentage of cost attributable to the processed product is determined using the first and second sets of information for use at the supply chain manager in operation **2336**.

In an aspect, the stores may include restaurants. In such an aspect, the processed product may include food. In another aspect, the first set of information may include an amount of the finished product. In a further aspect, the second set of information may include an amount of the processed product. In one aspect, the percentage may be made available utilizing a network-based interface.

Historical daily menu item sales data on a per store basis is the preferred backbone for all decision making and expanding analysis. Other causal information, variables that predict sales, can be collected and married with the menu item sales data to more accurately forecast. These variables might include weather, competitive information, marketing calendar, etc. Additional information such as menu item recipes can be used to further manipulate the data.

In a preferred embodiment, daily menu item sales data is received from restaurants on a per restaurant basis. This information is used to support the sales forecasting function and is used to report sales volumes to distributors and suppliers/manufacturers. Distributor level sales data is received on a weekly basis for all distributors, while supplier level sales data is received on a weekly basis for suppliers of "key products".

In order to best support real time supply chain management, access to information on product flow at the point of sale is provided on a daily basis. A representative sample of daily menu item sales can be collected if collection of all the data is not desired because of cumbersomeness, communications problems, etc.

Figure **24** is a flow diagram illustrating basic communication and product movement according to an illustrative embodiment of the present invention. As shown, orders and products move back and forth between suppliers **2402**, distributors **2404**, and restaurants **2406**. Daily menu item sales data is sent from the restaurants to restaurant management **2408**, where it is compiled and forwarded to the supply chain coordinator **2410**. The distributor sends periodic gross purchased by restaurant and item number to the supply chain coordinator. The supply chain coordinator also receives periodic invoice level sales data from the supplier.

Figure **25** is a flow diagram illustrating advanced communication and product movement according to an illustrative embodiment of the present invention. Again, orders and products move back and forth between suppliers **2502**, distributors **2504**, and restaurants **2506**. Daily menu item sales data is sent from the restaurants to restaurant management **2508**, where it is forwarded to the supply chain coordinator **2510**. The distributor sends invoice level sales information to the supply chain coordinator and receives daily product movement reports. The supply chain coordinator also receives invoice level sales data from the supplier and returns daily product movement reports to the supplier.

Figure **26** illustrates a Sales Forecast Worksheet **2600** that sets forth historical data **2602** and projected data **2604**. Figure **27** depicts a Promotion Monitoring Worksheet **2700** illustrating statistics **2702** such as variance from expected levels.

Figure **28** is a flowchart of a process **2830** for identifying goods in a network-based supply chain management framework. Data is generated at a plurality of stores of a supply chain utilizing a network in operation **2832**. The generated data relates to an ordering of goods required by the stores. The generated data is tagged with a numeric goods identifier common to a plurality of different supply chain participants in operation **2834**. The generated data and the numeric goods identifier are communicated via the network to one or more of the supply chain participants that are capable of using the data and the numeric goods identifier for fulfillment of the order in operation **2836**.

In one aspect, the numeric goods identifier may include a global trade identification number (GTIN). In another aspect, the generated data and the numeric goods identifier may be communicated utilizing a network-based interface. In a further aspect, the numeric goods identifier may actually be positioned on the goods. In such an aspect, the numeric goods identifier may be positioned on the goods in the form of a bar code. In another aspect, the generated data may be tagged by including the numeric goods identifier therewith. In yet another aspect, outlet information is communicated between the supply chain participants. Also, order information can be synchronized between supply chain providers.

Reports

Figure **29** is a flowchart of a process **2930** for generating supply chain statistics. Data is received utilizing a network from a plurality of stores, distributors and suppliers of a supply chain in operation **2932**. Preferably, the data is received from less than all of the stores, distributors and suppliers to generate closely-controlled representative statistics. The data is sampled in operation **2934** and supply chain statistics are generated based on the sampling in operation **2936**. The generated supply chain statistics are utilized for demand forecasting, advance planning, and/or volume tracking in the supply chain in operation **2938**.

In an aspect, the sampling may be representative of a predetermined percentage of the stores, distributors, and suppliers. In another aspect, the statistics may represent sales of the stores. In a further aspect, the statistics may represent goods ordered by the stores. In an additional aspect, the statistics may represent a timeliness of delivery of the ordered goods by the distributors. In one aspect, the statistics may represent an inventory of the suppliers.

Distributor

Figure **30** depicts a sample report **3000** for a distribution center. Measurements of operation performance are provided in an Operations section **3002** and include warehouse outs, damages, mispicks, short on truck, and overlooked and not returned. A Purchasing section **3004** includes statistics in Out of Stock, Substitutions, and Out of Code fields. Other sections of the report preferably include Delivery Order Fill Rate, On-time Delivery, Perfect Order Rate, and Price Compliance.

Figure **31** illustrates a Data Quality report **3100**. The report provides a comparison the following items to a group average: Bad Files, Late Files, No Files, and Time to Resolve.

Figure **32** illustrates a distributor ranking report **3200** that provides statistics on the number of orders filled, on-time deliveries, and perfect orders delivered, and whether they med the minimum required by the supply chain coordinator, retail management, or both.

Supplier

Figure **33** depicts a sample Supplier report **3300**. The report includes a Delivery Statistics section **3302** and other sections relating to Invoices and Inventory.

Figure **34** illustrates a Data Quality report **3400**. The report provides a comparison the following items to a group average: Bad Files, Late Files, No Files, and Time to Resolve.

Figure **35** illustrates a distributor ranking report **3500** that provides statistics on the number of orders filled, on-time deliveries, and perfect orders delivered, and whether they met the minimum required by the supply chain coordinator, retail management, or both.

Cost

Figure **36** illustrates a Food Cost Summary report **3600** that compares the actual cost of food against a projected cost.

Promotions

Figure **37** is a flowchart of a process **3730** for promotion reporting in a network-based supply chain management framework. Data associated with a promotion is identified in operation **3732**. Included in the data is promotion item information, location information, and duration information. A projected daily usage of the promotion item is calculated for a plurality of locations based on the data in operation **3734** and the projected daily usage of the promotion item is outputted utilizing a network with TCP/IP protocol in operation **3736**. Using this information, supplies can be shipped where they are needed, on a daily basis if need be. Further, the projected daily usage can be separated by region for statistical purposes.

In an aspect, each location may include a store. In another aspect, the calculating may include parsing the data based on location information and the promotion item, and dividing the data by the duration information. In a further aspect, the promotion items may include utensils. In yet another aspect, the promotion items may include food. In one aspect, the projected daily usage may be outputted via a network-based interface. In even another aspect, a projected daily usage of finished goods may also be calculated for the plurality of locations based on the data. Next, the projections may be translated into a

forecast of processed products required for the plurality of locations as well as into a forecast of delivery and storage parameters.

Confirmations

Figure **38** is a flowchart of a process **3830** for order confirmation in a supply chain management framework. A network is utilized in operation **3832** to collect from a plurality of stores of a supply chain data relating to the sale of goods by the stores. Access is allowed to the data utilizing a network-based interface in operation **3834**. Electronic order forms are generated in operation **3836** based on the data for ordering goods from a plurality of distributors of the supply chain. These electronic order forms request a confirmation of the receipt of the electronic order forms. A determination is made as to whether the confirmation of the receipt of the electronic order forms is received from the distributors in operation **3838**. If it is determined that the confirmation of the receipt of the electronic order forms was not from the distributors, then an alert is generated in operation **3840**.

In one aspect, the confirmation is received utilizing the network. In such an aspect, the network may include the Internet. In another aspect, the alert is transmitted to the stores utilizing the network. As an aspect, the alert may be displayed on the network-based interface. As a further aspect, the alert may include an electronic mail message.

Revenue Generation

The Supply Chain management system of the present invention creates, from its members, a web community with like interests. As a result, a number of different types of vendors may be interested in connecting to the site due to the captive audience comprising the web community, and because the community is a highly targeted audience with similar business goals/interests.

One area of revenue generation is collection of fees for advertising. Fees can be charged for such things as co-branding, local service and product providers, national providers of optional items/services, distributor specials, utilities, etc.

Revenue can also be generated by charging a fee to participants who buy and sell though the site, such as bakeries, soft drink vendors, coffee vendors, equipment vendors, consumers, restaurants, etc.

Sales and services can also be a source of revenue. Potential sources can be utilities, office products, computers, and equipment. Providing an auction service can also create revenue.

A preferred embodiment of the present invention utilizes one or more of the following revenue models: investment in web site, charge per unit sold through site, exposures or click through, or a combination of these.

Following are several processes for generating revenue.

Figure **39** is a flowchart of a process **3930** for advertising in a network-based supply chain management framework in which data is received utilizing a network from a plurality of stores of a supply chain in operation **3932**. A supply chain participant is allowed to access the data utilizing a network-based interface in operation **3934**. The supply chain participant accessing the network-based interface is identified in operation **3936** and advertising is presented to the supply chain participant in accordance with the identification in operation **3938**.

In an aspect, the network includes the Internet. In another aspect, the supply chain participant may be a supplier, a distributor, and/or a store. In such an aspect, the advertising advertises the sale of products required for the production of the goods produced by the stores. As another aspect, the advertising may be conducted by at least

one of the supply chain participants. In an additional aspect, a charge may be required for the advertising.

Figure **40** is a flowchart of a process **4030** for advertising in a network-based supply chain management framework. Data from a plurality of stores of a supply chain is received utilizing a network in operation **4032**. A supply chain participant is allowed to access the data utilizing a network-based interface in operation **4034**. The data being accessed by the supply chain participant is analyzed in operation **4036** so that advertising may be presented to the user in accordance with the analysis in operation **4038**.

In an aspect, the network includes the Internet. In another aspect, the supply chain participant may be a supplier, a distributor, and/or a store. In such an aspect, the advertising may advertise the sale of products required for the production of the goods produced by the stores. As another aspect, the advertising may be conducted by one of the supply chain participants. In one aspect, charge is required for the advertising.

Figure **41** is a flowchart of a process **4130** for generating revenue utilizing a network-based supply chain management framework. A network is utilized to receive data from a plurality of stores of a supply chain in operation **4132**. A user is allowed to access to the data utilizing a network-based interface in operation **4134**. Offers are then made to the user to sell products from a third party that are related to the store utilizing the network-based interface in operation **4136**. The third party is charged a fee based on a number of the products sold to the user utilizing the network-based interface in operation **4138**.

In one aspect, the network includes the Internet. In another aspect, the user may be a supplier, a distributor, and/or a store. In such an aspect, the products may be required for the production of the goods produced by the stores. In such an aspect, the advertising may be conducted by at least one of the users.

Figure **42** is a flowchart of a process **4230** for generating revenue utilizing a network-based supply chain management framework. Data is received via a network from a

plurality of stores of a supply chain in operation **4232**. A plurality of users are allowed to access the data utilizing a network-based interface in operation **4234**. The users are identified upon accessing the data utilizing the network-based interface in operation **4236** so that the users can be charged a fee based on a number of times the users access the data utilizing the network-based interface in operation **4238**.

In an aspect, the network includes the Internet. In one aspect, the users include suppliers, distributors, and/or stores. In another aspect, advertising is displayed on the network-based interface which advertises the sale of products required for the production of the goods produced by the store. As an aspect, the advertising may be conducted by at least one of the users. As another aspect, a charge is required for the advertising.

Figure **43A** is a flowchart of a process **4330** for an auction function utilizing a network-based supply chain management framework. Data is received via a network from a plurality of stores of a supply chain in operation **4332**. A plurality of users are allowed to access to the data utilizing a network-based interface in operation **4334**. A plurality of goods are displayed to the users accessing the data utilizing the network-based interface in operation **4336**. Subsequently, the acceptance of bids on the goods is allowed from the users utilizing the network in operation **4338**.

In one aspect, the network includes the Internet. In another aspect, the users may be a supplier, a distributor, and/or a store. In a further aspect, advertising is displayed on the network-based interface which advertises the sale of products required for the production of the goods produced by the store. In such an aspect, the advertising may be conducted by at least one of the users. As another aspect, a charge may be required for the advertising.

Figure **43B** is a flow diagram of a process **4350** for utilizing market demand information for generating revenue. In operation **4352**, a supply chain manager is appointed for at least one buying supply chain participant. Such appointment can be made arbitrarily, by default, upon selection by the supply chain participant, etc. In operation **4354**, a grant of

authority is given to the supply chain manager to negotiate purchase agreements for at least one supply chain commodity on behalf of the at least one buying supply chain participant. One or more purchase agreements for the commodity are entered into in operation **4356**. Each purchase agreement is between the supply chain manager on behalf of the at least one buying supply chain participant and a selling supply chain participant. A periodic analysis of commodity market price information is performed in operation **4358**. Such price information includes information derived from an integrated supply management system for determining an effective price of the commodity. In the purchase agreement(s), a contract price that depends upon the effective price for the commodity is established in operation **4360** in circumstances where a determination of the effective price of the commodity has been made.

In one aspect, the supply chain manager is granted authority to negotiate purchase agreements for the at least one supply chain commodity on behalf of all buying supply chain participants. The commodity can be a raw material, a partially finished good, and/or a finished good. In a further aspect, the at least one purchase agreement establishes a contract price depending upon an actual market price for the commodity in circumstances where no determination of the effective price of the commodity has been made. In one aspect, an actual market price of the commodity is kept secret from the at least one buying supply chain participant. In another aspect, an identity of the at least one buying supply chain participant is kept secret from a supplier of the commodity.

One benefit of this embodiment of the present invention is that the supply chain manager may have greater information about market demand for various raw material commodities than a distributor, and may wish to benefit from the availability of this information. By fixing an "effective raw material price," the supplier is free to either take the required position (at no cost, since the contract price will be based upon the effective price), or take a contrary view, with the associated risk and benefit.

An additional benefit of this system is that the supply chain manager may exploit raw material information without: (1) disclosing confidential information beyond the fixed

price analysis; and (2) needing to include raw material suppliers immediately into the integrated supply chain models.

Figure **43C** is a flow diagram of another process **4370** for generating revenue according to an embodiment of the present invention. A supply chain manager is appointed for a buying supply chain participant in operation **4372**. In operation **4374**, authority is granted to the supply chain manager to negotiate supply agreements between a selling supply chain participant and the supply chain manager on behalf of the buying supply chain participant. The supply agreement is entered into with the supply agreement having at least the following provisions: i) establishing a contract price for the good, and ii) requiring the selling supply chain participant to bill the buying supply chain participant at an invoice price to be determined by the supply chain manager in operation **4376**. In operation **4378**, an invoice price for the good is established at various times during the term of the supply agreement.

By controlling the invoice price, the distributor does not know the contract price of the supplier. Another advantage provided is that the supply chain manager can direct supplier to buy raw materials at a particular price based on supply and demand information gathered by the supply chain management system.

In one aspect of the present invention, the invoice price is collected from the buying supply chain participant(s). Preferably, the billing and collecting are performed at the direction of the supply chain manager. In another aspect, an overpayment to a selling supply chain participant for a commodity is reconciled by paying the difference between the corresponding contract price and the corresponding invoice price to the supply chain manager. In a further aspect, an underpayment to a selling supply chain participant for a commodity is reconciled by paying the difference between the corresponding invoice price and the corresponding contract price to the selling supply chain participant.

Figure **43D** is a flow chart of a process **4386** for risk management in a supply chain management framework. In operation **4388**, a supply chain manager is appointed for at

least one buying supply chain participant. Such appointment can be made arbitrarily, by default, upon selection by the supply chain participant, etc. In operation **4390**, the supply chain manager is given authority to negotiate supply agreements for at least one good on behalf of the at least one buying supply chain participant. Note that the good may be a raw material and/or a fully finished good as well. One or more supply agreements are entered into for the at least one good in operation **4392**. Provisions of the supply agreement include: (i) pricing for each one good shall be based upon factors including an actual market price of at least one commodity when the supply chain manager has not established a commodity position price; and (ii) pricing for each one good shall be based upon factors including a commodity position price of at least one commodity when the supply chain manager has established a commodity position price. Periodically, in operation **4394**, a commodity position price is established through the supply chain manager, so that the supply chain manager may thereby address risks to the supply chain of varying market levels and market volatility of the at least one goods.

In one aspect of the present invention, commodity position prices can be established based on information including information derived from receiving data from a plurality of supply chain participants of a supply chain utilizing a network, the data relating to the sale of products by the supply chain participants.

In one aspect, the supply chain manager is granted authority to negotiate supply agreements for the at least one good on behalf of all buying supply chain participants. In another aspect, an actual market price of the at least one good is kept secret from the at least one buying supply chain participant. In a further aspect, an identity of the at least one buying supply chain participant is kept secret from a supplier of the at least one good. In yet another aspect, each supply agreement is between the supply chain manager on behalf of the at least one buying supply chain participant and a selling supply chain participant. In even a further aspect, the good may be an at least partially finished good. In an additional aspect, the determining may include the analyzing of data collected from a plurality of supply chain participants relating to the sale of goods.

Technology Overview

Figure **44** illustrates an exemplary system **4400** with a plurality of components **4402** in accordance with one embodiment of the present invention. As shown, such components include a network **4404** which take any form including, but not limited to a local area network, a wide area network such as the Internet, and a wireless network **4405**. Coupled to the network **4404** is a plurality of computers which may take the form of desktop computers **4406**, lap-top computers **4408**, hand-held computers **4410** (including wireless devices **4412** such as wireless PDA's or mobile phones), or any other type of computing hardware/software. As an option, the various computers may be connected to the network **4404** by way of a server **4414** which may be equipped with a firewall for security purposes. It should be noted that any other type of hardware or software may be included in the system and be considered a component thereof.

A representative hardware environment associated with the various components of Figure **44** is depicted in Figure **45**. In the present description, the various sub-components of each of the components may also be considered components of the system. For example, particular software modules executed on any component of the system may also be considered components of the system. Figure **45** illustrates a typical hardware configuration of a workstation in accordance with one embodiment having a central processing unit **4510**, such as a microprocessor, and a number of other units interconnected via a system bus **4512**.

The workstation shown in Figure **45** includes a Random Access Memory (RAM) **4514**, Read Only Memory (ROM) **4516**, an I/O adapter **4518** for connecting peripheral devices such as disk storage units **4520** to the bus **512**, a user interface adapter **4522** for connecting a keyboard **4524**, a mouse **4526**, a speaker **4528**, a microphone **4532**, and/or other user interface devices such as a touch screen (not shown) to the bus **4512**, communication adapter **4534** for connecting the workstation to a communication network **4535** (e.g., a data processing network) and a display adapter **4536** for connecting the bus **4512** to a display device **4538**.

An embodiment of the present invention may be written using traditional methodologies and programming languages, such as C, Pascal, BASIC or Fortran, or may be written using object oriented methodologies and object-oriented programming languages, such as Java, C++, C#, Python or Smalltalk. Object oriented programming (OOP) has become increasingly used to develop complex applications. As OOP moves toward the mainstream of software design and development, various software solutions require adaptation to make use of the benefits of OOP. A need exists for these principles of OOP to be applied to a messaging interface of an electronic messaging system such that a set of OOP classes and objects for the messaging interface can be provided.

OOP is a process of developing computer software using objects, including the steps of analyzing the problem, designing the system, and constructing the program. An object is a software package that contains both data and a collection of related structures and procedures. Since it contains both data and a collection of structures and procedures, it can be visualized as a self-sufficient component that does not require other additional structures, procedures or data to perform its specific task. OOP, therefore, views a computer program as a collection of largely autonomous components, called objects, each of which is responsible for a specific task. This concept of packaging data, structures, and procedures together in one component or module is called encapsulation.

In general, OOP components are reusable software modules which present an interface that conforms to an object model and which are accessed at run-time through a component integration architecture. A component integration architecture is a set of architecture mechanisms which allow software modules in different process spaces to utilize each others capabilities or functions. This is generally done by assuming a common component object model on which to build the architecture. It is worthwhile to differentiate between an object and a class of objects at this point. An object is a single instance of the class of objects, which is often just called a class. A class of objects can be viewed as a blueprint, from which many objects can be formed.

OOP allows the programmer to create an object that is a part of another object. For example, the object representing a piston engine is said to have a composition-relationship with the object representing a piston. In reality, a piston engine comprises a piston, valves and many other components; the fact that a piston is an element of a piston engine can be logically and semantically represented in OOP by two objects.

OOP also allows creation of an object that "depends from" another object. If there are two objects, one representing a piston engine and the other representing a piston engine wherein the piston is made of ceramic, then the relationship between the two objects is not that of composition. A ceramic piston engine does not make up a piston engine. Rather it is merely one kind of piston engine that has one more limitation than the piston engine; its piston is made of ceramic. In this case, the object representing the ceramic piston engine is called a derived object, and it inherits all of the aspects of the object representing the piston engine and adds further limitation or detail to it. The object representing the ceramic piston engine "depends from" the object representing the piston engine. The relationship between these objects is called inheritance.

When the object or class representing the ceramic piston engine inherits all of the aspects of the objects representing the piston engine, it inherits the thermal characteristics of a standard piston defined in the piston engine class. However, the ceramic piston engine object overrides these ceramic specific thermal characteristics, which are typically different from those associated with a metal piston. It skips over the original and uses new functions related to ceramic pistons. Different kinds of piston engines have different characteristics, but may have the same underlying functions associated with it (e.g., how many pistons in the engine, ignition sequences, lubrication, etc.). To access each of these functions in any piston engine object, a programmer would call the same functions with the same names, but each type of piston engine may have different/overriding implementations of functions behind the same name. This ability to hide different implementations of a function behind the same name is called polymorphism and it greatly simplifies communication among objects.

With the concepts of composition-relationship, encapsulation, inheritance and polymorphism, an object can represent just about anything in the real world. In fact, one's logical perception of the reality is the only limit on determining the kinds of things that can become objects in object-oriented software. Some typical categories are as follows:

- Objects can represent physical objects, such as automobiles in a traffic-flow simulation, electrical components in a circuit-design program, countries in an economics model, or aircraft in an air-traffic-control system.
- Objects can represent elements of the computer-user environment such as windows, menus or graphics objects.
- An object can represent an inventory, such as a personnel file or a table of the latitudes and longitudes of cities.
- An object can represent user-defined data types such as time, angles, and complex numbers, or points on the plane.

With this enormous capability of an object to represent just about any logically separable matters, OOP allows the software developer to design and implement a computer program that is a model of some aspects of reality, whether that reality is a physical entity, a process, a system, or a composition of matter. Since the object can represent anything, the software developer can create an object which can be used as a component in a larger software project in the future.

If 90% of a new OOP software program consists of proven, existing components made from preexisting reusable objects, then only the remaining 10% of the new software project has to be written and tested from scratch. Since 90% already came from an inventory of extensively tested reusable objects, the potential domain from which an error could originate is 10% of the program. As a result, OOP enables software developers to build objects out of other, previously built objects.

This process closely resembles complex machinery being built out of assemblies and sub-assemblies. OOP technology, therefore, makes software engineering more like hardware

engineering in that software is built from existing components, which are available to the developer as objects. All this adds up to an improved quality of the software as well as an increased speed of its development.

Programming languages are beginning to fully support the OOP principles, such as encapsulation, inheritance, polymorphism, and composition-relationship. With the advent of the C++ language, many commercial software developers have embraced OOP. C++ is an OOP language that offers a fast, machine-executable code. Furthermore, C++ is suitable for both commercial-application and systems-programming projects. For now, C++ appears to be the most popular choice among many OOP programmers, but there is a host of other OOP languages, such as Smalltalk, Common Lisp Object System (CLOS), and Eiffel. Additionally, OOP capabilities are being added to more traditional popular computer programming languages such as Pascal.

The benefits of object classes can be summarized, as follows:

- Objects and their corresponding classes break down complex programming problems into many smaller, simpler problems.
- Encapsulation enforces data abstraction through the organization of data into small, independent objects that can communicate with each other. Encapsulation protects the data in an object from accidental damage, but allows other objects to interact with that data by calling the object's member functions and structures.
- Subclassing and inheritance make it possible to extend and modify objects through deriving new kinds of objects from the standard classes available in the system. Thus, new capabilities are created without having to start from scratch.
- Polymorphism and multiple inheritance make it possible for different programmers to mix and match characteristics of many different classes and create specialized objects that can still work with related objects in predictable ways.
- Class hierarchies and containment hierarchies provide a flexible mechanism for modeling real-world objects and the relationships among them.

- Libraries of reusable classes are useful in many situations, but they also have some limitations. For example:
- Complexity. In a complex system, the class hierarchies for related classes can become extremely confusing, with many dozens or even hundreds of classes.
- Flow of control. A program written with the aid of class libraries is still responsible for the flow of control (i.e., it must control the interactions among all the objects created from a particular library). The programmer has to decide which functions to call at what times for which kinds of objects.
- Duplication of effort. Although class libraries allow programmers to use and reuse many small pieces of code, each programmer puts those pieces together in a different way. Two different programmers can use the same set of class libraries to write two programs that do exactly the same thing but whose internal structure (i.e., design) may be quite different, depending on hundreds of small decisions each programmer makes along the way. Inevitably, similar pieces of code end up doing similar things in slightly different ways and do not work as well together as they should.

Class libraries are very flexible. As programs grow more complex, more programmers are forced to reinvent basic solutions to basic problems over and over again. A relatively new extension of the class library concept is to have a framework of class libraries. This framework is more complex and consists of significant collections of collaborating classes that capture both the small scale patterns and major mechanisms that implement the common requirements and design in a specific application domain. They were first developed to free application programmers from the chores involved in displaying menus, windows, dialog boxes, and other standard user interface elements for personal computers.

Frameworks also represent a change in the way programmers think about the interaction between the code they write and code written by others. In the early days of procedural programming, the programmer called libraries provided by the operating system to perform certain tasks, but basically the program executed down the page from start to

finish, and the programmer was solely responsible for the flow of control. This was appropriate for printing out paychecks, calculating a mathematical table, or solving other problems with a program that executed in just one way.

The development of graphical user interfaces began to turn this procedural programming arrangement inside out. These interfaces allow the user, rather than program logic, to drive the program and decide when certain actions should be performed. Today, most personal computer software accomplishes this by means of an event loop which monitors the mouse, keyboard, and other sources of external events and calls the appropriate parts of the programmer's code according to actions that the user performs. The programmer no longer determines the order in which events occur. Instead, a program is divided into separate pieces that are called at unpredictable times and in an unpredictable order. By relinquishing control in this way to users, the developer creates a program that is much easier to use. Nevertheless, individual pieces of the program written by the developer still call libraries provided by the operating system to accomplish certain tasks, and the programmer must still determine the flow of control within each piece after it's called by the event loop. Application code still "sits on top of" the system.

Even event loop programs require programmers to write a lot of code that should not need to be written separately for every application. The concept of an application framework carries the event loop concept further. Instead of dealing with all the nuts and bolts of constructing basic menus, windows, and dialog boxes and then making these things all work together, programmers using application frameworks start with working application code and basic user interface elements in place. Subsequently, they build from there by replacing some of the generic capabilities of the framework with the specific capabilities of the intended application.

Application frameworks reduce the total amount of code that a programmer has to write from scratch. However, because the framework is really a generic application that displays windows, supports copy and paste, and so on, the programmer can also relinquish control to a greater degree than event loop programs permit. The framework

code takes care of almost all event handling and flow of control, and the programmer's code is called only when the framework needs it (e.g., to create or manipulate a proprietary data structure).

A programmer writing a framework program not only relinquishes control to the user (as is also true for event loop programs), but also relinquishes the detailed flow of control within the program to the framework. This approach allows the creation of more complex systems that work together in interesting ways, as opposed to isolated programs, having custom code, being created over and over again for similar problems.

Thus, as is explained above, a framework basically is a collection of cooperating classes that make up a reusable design solution for a given problem domain. It typically includes objects that provide default behavior (e.g., for menus and windows), and programmers use it by inheriting some of that default behavior and overriding other behavior so that the framework calls application code at the appropriate times.

There are three main differences between frameworks and class libraries:

- Behavior versus protocol. Class libraries are essentially collections of behaviors that can be called when those individual behaviors are desired in the program. A framework, on the other hand, provides not only behavior but also the protocol or set of rules that govern the ways in which behaviors can be combined, including rules for what a programmer is supposed to provide versus what the framework provides.
- Call versus override. With a class library, the code the programmer instantiates objects and calls their member functions. It's possible to instantiate and call objects in the same way with a framework (i.e., to treat the framework as a class library), but to take full advantage of a framework's reusable design, a programmer typically writes code that overrides and is called by the framework. The framework manages the flow of control among its objects. Writing a program involves dividing responsibilities among the various pieces of software

that are called by the framework rather than specifying how the different pieces should work together.

- Implementation versus design. With class libraries, programmers reuse only implementations, whereas with frameworks, they reuse design. A framework embodies the way a family of related programs or pieces of software work. It represents a generic design solution that can be adapted to a variety of specific problems in a given domain. For example, a single framework can embody the way a user interface works, even though two different user interfaces created with the same framework might solve quite different interface problems.

Thus, through the development of frameworks for solutions to various problems and programming tasks, significant reductions in the design and development effort for software can be achieved. A preferred embodiment of the invention utilizes HyperText Markup Language (HTML) to implement documents on the Internet together with a general-purpose secure communication protocol for a transport medium between the client and the server. Information on these products is available in T. Berners-Lee, D. Connoly, "RFC 1866: Hypertext Markup Language - 2.0" (Nov. 1995); and R. Fielding, H, Frystyk, T. Berners-Lee, J. Gettys and J.C. Mogul, "Hypertext Transfer Protocol -- HTTP/1.1: HTTP Working Group Internet Draft" (May 2, 1996). HTML is a simple data format used to create hypertext documents that are portable from one platform to another. SGML documents are documents with generic semantics that are appropriate for representing information from a wide range of domains and are HTML compatible. HTML has been in use by the World-Wide Web global information initiative since 1990. HTML is an application of ISO Standard 8879; 1986 Information Processing Text and Office Systems; Standard Generalized Markup Language (SGML).

XML (Extensible Markup Language) is a flexible way to create common information formats and share both the format and the data on the World Wide Web, intranets, and elsewhere. For example, computer makers might agree on a standard or common way to describe the information about a computer product (processor speed, memory size, and so forth) and then describe the product information format with XML. Such a standard way

of describing data would enable a user to send an intelligent agent (a program) to each computer maker's Web site, gather data, and then make a valid comparison. XML can be used by any individual or group of individuals or companies that wants to share information in a consistent way.

XML, a formal recommendation from the World Wide Web Consortium (W3C), is similar to the language of today's Web pages, the Hypertext Markup Language (HTML). Both XML and HTML contain markup symbols to describe the contents of a page or file. HTML, however, describes the content of a Web page (mainly text and graphic images) only in terms of how it is to be displayed and interacted with. For example, the letter "p" placed within markup tags starts a new paragraph. XML describes the content in terms of what data is being described. For example, the word "phonenum" placed within markup tags could indicate that the data that followed was a phone number. This means that an XML file can be processed purely as data by a program or it can be stored with similar data on another computer or, like an HTML file, that it can be displayed. For example, depending on how the application in the receiving computer wanted to handle the phone number, it could be stored, displayed, or dialed.

XML is "extensible" because, unlike HTML, the markup symbols are unlimited and self-defining. XML is actually a simpler and easier-to-use subset of the Standard Generalized Markup Language (SGML), the standard for how to create a document structure. It is expected that HTML and XML will be used together in many Web applications. XML markup, for example, may appear within an HTML page.

To date, Web development tools have been limited in their ability to create dynamic Web applications which span from client to server and interoperate with existing computing resources. Until recently, HTML has been the dominant technology used in development of Web-based solutions. However, HTML has proven to be inadequate in the following areas:

- Poor performance;
- Restricted user interface capabilities;

- Can only produce static Web pages;
- Lack of interoperability with existing applications and data; and
- Inability to scale.

Sun Microsystems's Java language solves many of the client-side problems by:

- Improving performance on the client side;
- Enabling the creation of dynamic, real-time Web applications; and
- Providing the ability to create a wide variety of user interface components.

With Java, developers can create robust User Interface (UI) components. Custom "widgets" (e.g., real-time stock tickers, animated icons, etc.) can be created, and client-side performance is improved. Unlike HTML, Java supports the notion of client-side validation, offloading appropriate processing onto the client for improved performance. Dynamic, real-time Web pages can be created. Using the above-mentioned custom UI components, dynamic Web pages can also be created.

Sun's Java language has emerged as an industry-recognized language for "programming the Internet." Sun defines Java as: "a simple, object-oriented, distributed, interpreted, robust, secure, architecture-neutral, portable, high-performance, multithreaded, dynamic, buzzword-compliant, general-purpose programming language. Java supports programming for the Internet in the form of platform-independent Java applets." Java applets are small, specialized applications that comply with Sun's Java Application Programming Interface (API) allowing developers to add "interactive content" to Web documents (e.g., simple animations, page adornments, basic games, etc.). Applets execute within a Java-compatible browser (e.g., Netscape Navigator) by copying code from the server to client. From a language standpoint, Java's core feature set is based on C++. Sun's Java literature states that Java is basically, "C++ with extensions from Objective C for more dynamic method resolution."

Another technology that provides similar function to Java is provided by Microsoft and ActiveX Technologies, to give developers and Web designers wherewithal to build

dynamic content for the Internet and personal computers. ActiveX includes tools for developing animation, 3-D virtual reality, video and other multimedia content. The tools use Internet standards, work on multiple platforms, and are being supported by over 100 companies. The group's building blocks are called ActiveX Controls, small, fast components that enable developers to embed parts of software in hypertext markup language (HTML) pages. ActiveX Controls work with a variety of programming languages including Microsoft Visual C++, Borland Delphi, Microsoft Visual Basic programming system and, in the future, Microsoft's development tool for Java, code named "Jakarta." ActiveX Technologies also includes ActiveX Server Framework, allowing developers to create server applications. One of ordinary skill in the art readily recognizes that ActiveX could be substituted for Java without undue experimentation to practice the invention.

Transmission Control Protocol/Internet Protocol (TCP/IP) is a basic communication language or protocol of the Internet. It can also be used as a communications protocol in the private networks called intranet and in extranet. When one is set up with direct access to the Internet, his or her computer is provided with a copy of the TCP/IP program just as every other computer that he or she may send messages to or get information from also has a copy of TCP/IP.

TCP/IP comprises a Transmission Control Protocol (TCP) layer and an Internet Protocol (IP) layer. TCP manages the assembling of series of packets from a message or file for transmission of packets over the internet from a source host to a destination host. IP handles the addressing of packets to provide for the delivery of each packet from the source host to the destination host. Host computers on a network, receive packets analyze the addressing of the packet If the host computer is not the destination the host attempts to route the packet by forwarding it to another host that is closer in some sense to the packet's destination. While some packets may be routed differently through a series of interim host computers than others, TCP and IP provides for the packets to be correctly reassembled at the ultimate destination.

TCP/IP uses a client/server model of communication in which a computer user (a client) requests and is provided a service (such as sending a Web page) by another computer (a server) in the network. TCP/IP communication is primarily point-to-point, meaning each communication is from one point (or host computer) in the network to another point or host computer. TCP/IP and the higher-level applications that use it are collectively said to be "stateless" because each client request is considered a new request unrelated to any previous one (unlike ordinary phone conversations that require a dedicated connection for the call duration). Being stateless frees network paths so that everyone can use them continuously (note that the TCP layer itself is not stateless as far as any one message is concerned. Its connection remains in place until all packets in a message have been received.).

Many Internet users are familiar with the even higher layer application protocols that use TCP/IP to get to the Internet. These include the World Wide Web's Hypertext Transfer Protocol (HTTP), the File Transfer Protocol (FTP), Telnet which lets one logon to remote computers, and the Simple Mail Transfer Protocol (SMTP). These and other protocols are often packaged together with TCP/IP as a "suite."

Personal computer users usually get to the Internet through the Serial Line Internet Protocol (SLIP) or the Point-to-Point Protocol. These protocols encapsulate the IP packets so that they can be sent over a dial-up phone connection to an access provider's modem.

Protocols related to TCP/IP include the User Datagram Protocol (UDP), which is used instead of TCP for special purposes. Other protocols are used by network host computers for exchanging router information. These include the Internet Control Message Protocol (ICMP), the Interior Gateway Protocol (IGP), the Exterior Gateway Protocol (EGP), and the Border Gateway Protocol (BGP).

Internetwork Packet Exchange (IPX)is a networking protocol from Novell that interconnects networks that use Novell's NetWare clients and servers. IPX is a datagram

or packet protocol. IPX works at the network layer of communication protocols and is connectionless (that is, it doesn't require that a connection be maintained during an exchange of packets as, for example, a regular voice phone call does).

Packet acknowledgment is managed by another Novell protocol, the Sequenced Packet Exchange (SPX). Other related Novell NetWare protocols are: the Routing Information Protocol (RIP), the Service Advertising Protocol (SAP), and the NetWare Link Services Protocol (NLSP).

A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. A virtual private network can be contrasted with a system of owned or leased lines that can only be used by one company. The idea of the VPN is to give the company the same capabilities at much lower cost by using the shared public infrastructure rather than a private one. Phone companies have provided secure shared resources for voice messages. A virtual private network makes it possible to have the same secure sharing of public resources for data.

Using a virtual private network involves encryption data before sending it through the public network and decrypting it at the receiving end. An additional level of security involves encrypting not only the data but also the originating and receiving network addresses. Microsoft, 3Com, and several other companies have developed the Point-to-Point Tunneling Protocol (PPTP) and Microsoft has extended Windows NT to support it. VPN software is typically installed as part of a company's firewall server.

Wireless refers to a communications, monitoring, or control system in which electromagnetic radiation spectrum or acoustic waves carry a signal through atmospheric space rather than along a wire. In most wireless systems, radio frequency (RF) or infrared transmission (IR) waves are used. Some monitoring devices, such as intrusion alarms, employ acoustic waves at frequencies above the range of human hearing.

Early experimenters in electromagnetic physics dreamed of building a so-called wireless telegraph. The first wireless telegraph transmitters went on the air in the early years of the 20th century. Later, as amplitude modulation (AM) made it possible to transmit voices and music via wireless, the medium came to be called radio. With the advent of television, fax, data communication, and the effective use of a larger portion of the electromagnetic spectrum, the original term has been brought to life again.

Common examples of wireless equipment in use today include the Global Positioning System, cellular telephone phones and pagers, cordless computer accessories (for example, the cordless mouse), home-entertainment-system control boxes, remote garage-door openers, two-way radios, and baby monitors. An increasing number of companies and organizations are using wireless LAN. Wireless transceivers are available for connection to portable and notebook computers, allowing Internet access in selected cities without the need to locate a telephone jack. Eventually, it will be possible to link any computer to the Internet via satellite, no matter where in the world the computer might be located.

Bluetooth is a computing and telecommunications industry specification that describes how mobile phones, computers, and personal digital assistants (PDA's) can easily interconnect with each other and with home and business phones and computers using a short-range wireless connection. Each device is equipped with a microchip transceiver that transmits and receives in a previously unused frequency band of 2.45 GHz that is available globally (with some variation of bandwidth in different countries). In addition to data, up to three voice channels are available. Each device has a unique 48-bit address from the IEEE 802 standard. Connections can be point-to-point or multipoint. The maximum range is 10 meters. Data can be presently be exchanged at a rate of 1 megabit per second (up to 2 Mbps in the second generation of the technology). A frequency hop scheme allows devices to communicate even in areas with a great deal of electromagnetic interference. Built-in encryption and verification is provided.

Encryption is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.

The use of encryption/decryption is as old as the art of communication. In wartime, a cipher, often incorrectly called a "code," can be employed to keep the enemy from obtaining the contents of transmissions (technically, a code is a means of representing a signal without the intent of keeping it secret; examples are Morse code and ASCII). Simple ciphers include the substitution of letters for numbers, the rotation of letters in the alphabet, and the "scrambling" of voice signals by inverting the sideband frequencies. More complex ciphers work according to sophisticated computer algorithm that rearrange the data bits in digital signals.

In order to easily recover the contents of an encrypted signal, the correct decryption key is required. The key is an algorithm that "undoes" the work of the encryption algorithm. Alternatively, a computer can be used in an attempt to "break" the cipher. The more complex the encryption algorithm, the more difficult it becomes to eavesdrop on the communications without access to the key.

Rivest-Shamir-Adleman (RSA) is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is a commonly used encryption and authentication algorithm and is included as part of the Web browser from Netscape and Microsoft. It's also part of Lotus Notes, Intuit's Quicken, and many other products. The encryption system is owned by RSA Security.

The RSA algorithm involves multiplying two large prime numbers (a prime number is a number divisible only by that number and 1) and through additional operations deriving a set of two numbers that constitutes the public key and another set that is the private key. Once the keys have been developed, the original prime numbers are no longer important and can be discarded. Both the public and the private keys are needed for encryption

/decryption but only the owner of a private key ever needs to know it. Using the RSA system, the private key never needs to be sent across the Internet.

The private key is used to decrypt text that has been encrypted with the public key. Thus, if User A sends User B a message, User A can find out User B's public key (but not User B's private key) from a central administrator and encrypt a message to User B using User B's public key. When User B receives it, User B decrypts it with User B's private key. In addition to encrypting messages (which ensures privacy), User B can authenticate himself to User A (so User A knows that it is really User B who sent the message) by using User B's private key to encrypt a digital certificate. When User A receives it, User A can use User B's public key to decrypt it.

Communication

Data collection and dissemination is preferably accomplished over a network such as the Internet.

Figure **46** is a flowchart of a process **4630** for providing network-based supply chain communication between participants in the supply chain such as stores, distributors, suppliers, a supply chain manager, and an office of the supply chain manager. Invoice level sales data is transmitted from the supplier to the supply chain manager utilizing a network in operation **4632**. Gross purchase data is sent from the distributors to the supply chain manager utilizing the network in operation **4634**. Daily sales data is communicated from the stores to the office of the supply chain manager utilizing the network in operation **4636** and total menu item sales data is transmitted from the office of the supply chain manager to the supply chain manager utilizing the network in operation **4638**.

In an aspect, the network includes the Internet. In another aspect, the stores, the distributors, the suppliers, the supply chain manager, and the office of the supply chain manager communicate utilizing a network-based interface. In a further aspect, the gross

purchase data includes monthly gross purchase data. In one aspect, the supply chain manager manages the distributors.

Figure **47** is a flowchart of a process **4730** for providing network-based supply chain communication between participants in the supply chain such as stores, distributors, suppliers, a supply chain manager, and an office of the supply chain manager. Invoice level sales data is transmitted from the supplier to the supply chain manager utilizing a network in operation **4732**. Invoice level sales data is sent from the distributors to the supply chain manager utilizing the network in operation **4734**. Daily sales data is communicated from the stores to the office of the supply chain manager utilizing the network in operation **4736**. Daily sales data is transmitted from the office of the supply chain manager to the supply chain manager utilizing the network in operation **4738**. The daily sales data is organized based on the stores from which the daily sales data originated.

In one aspect, the network includes the Internet. In another aspect, the stores, the distributors, the suppliers, the supply chain manager, and the office of the supply chain manager communicate utilizing a network-based interface. In a further aspect, the gross purchase data includes monthly gross purchase data. In an additional aspect, the supply chain manager manages the distributors.

EMail Capability

An E-mail system can be used to report information if external mail capabilities that support the Internet are present. Any existing Internet account can be used, as can one from a value added service provider (e.g. America On-line, Compuserv, Microsoft Network, etc.). If there are no existing E-Mail capabilities, an account can be established with an Internet Service Provider.

SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it's limited in its ability to queue messages at the

receiving end, it's usually used with one of two other protocols, POP3 or Internet Message Access Protocol, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving messages that have been received for them at their local server. Most mail programs such as Eudora let you specify both an SMTP server and a POP server. On UNIX-based systems, sendmail is the most widely-used SMTP server for e-mail. A commercial package, Sendmail, includes a POP3 server and also comes in a version for Windows NT.

The next step is testing E-mail connectivity by sending a message to Supply Chain management's Test Mailbox. A response is made (via other communications means) in the event the E-mail transmission is not received. A reply to the message via E-mail is made once successfully received. As an option, a file attachment (any text-ASCII file) can be included to verify the ability to send messages with separate file attachments.

After receiving confirmation concerning a successful Test Message, an actual data file (created from the *Franchisee Information Layout* section, below) is sent to the TEST Mailbox. After receiving confirmation concerning successful processing of the Test data, a notification is sent to begin Production reporting according to the reporting period specified in the *Franchisee Information Layout* section.

Franchisee Information Layout

Table 1 sets forth Illustrative daily POS data elements

Table 1

Fld #	Data Element Name	Type	Size	Column(s)	Example	Req
00	Record Type	ID	3	001-003	FR1	M
01	Item Number	ID	10	004-013	12645	M

02	Item Description	AN	20	014-033	burger patty	M
03	Period Date	DT	8	034-041	19990601	M
04	Retail Outlet Number	ID	4	042-045	0107	M
05	Total Sales $	N2	6	046-051	3264.50	M
06	Total Quantity	NO	5	052-056	1034	M

Example: This example should be one line. Field justification is irrelevant.

```
          1         2         3         4         5
5 12345678901234567890123456789012345678901234567890123456
  FR112645  whopper patty          199906010107326450 1034
```

General Implementation Information

10 The following information is a guideline for the requested data files.

Record Type:

All records that are similar are considered a logical group of data. Each record in a group
15 has a unique identifier called a Record Type consisting of three alphanumeric characters. This should be placed before the first field of each record (see the Example above in the *Franchisee Information Layout* section), and repeated on each row.

Field:

20

A Field can represent a qualifier, a value, or text (such as a description). A Field can be thought of as a piece of data.

Record:

25

Each row of data is a Record. To allow for future expansion, Records can be padded to any length.

Field Number:

Based upon the sequential position assignment of a Field in the Record, each Field assumes a unique or numeric location for each Record. The value of the FLD# column represents the position within the Record where the individual Field appears (i.e., FLD#01 will be the first Field following the Record Type, FLD#02 will be the second Field following the Record Type, etc.).

Fields:

Fields can be either left or right justified. The Record Type should always precede the first field. All Fields should completely fill their column sizes (pad with spaces).

Field Types:

AN	Alpha/Numeric - Should not be enclosed in quotes (e.g. FXD-4543).
Nn	Numeric with n decimal places - Symbolized by the two-position representation Nn. N indicates a numeric, and n indicates the decimal places to the right of a fixed decimal point. This should not contain dollar signs or commas, but may contain decimal points (e.g. N2 for $4,255.50 is 4255.50; N0 for $4,255.50 is 4256). This should be rounded to the respective decimal place (e.g. N2 for $4,255.506 is 4255.51). For negative values, a leading minus sign (-) is used (e.g. N2 for $-12.42 is -12.42). Left-padding with zeroes is optional (e.g. 4532 could be either 4532 or 004532).

ID — Identifier Value - May contain alpha/numeric data restricted to a list of possible values.

DT — Date Value - Format for the date type is CCYYMMDD, where CC indicates century, YY is the last two digits of the year (00-99), MM is the numeric value of the month (01-12), and DD is the numeric value of the day (01-31).

TM — Time Value - Format for the time type is HHMMSS. HH is the numeric expression of the hour (00-23), MM is the numeric expression of the minute (00-59), SS is the numeric expression of the second (00-59), and d..d is the numeric expression of the decimal seconds. This fields may be relevant for EDI formats.

Size:

The minus sign and the decimal point are counted when determining the length of the data element (Field) value.

Column(s):

Specifies the column numbers allocated to a particular Field.

Requirement (Req):

M	Mandatory	This field must be present
C	Conditional	This field is present based on a condition
O	Optional	This field may become Mandatory or
R	Reserved	Reserved for future use

File Format.

All files can be requested in a fixed-length ASCII format. Programmatically, these are simple to produce. Many PC applications include an export utility which allows specification of column widths and formats. When using spreadsheet applications, column widths and formats may have to be pre-set to produce the desired results. Empty Fields can be filled with spaces.

Compression.

Files can be compressed. Compressing files will typically reduce file sizes to some 20% of their initial size. Preferably, the system supports the use of ZIP files created from a PC. Before transmission, all files would be compressed into one ZIP file using PKZIP, a file compression package available from most software sources.

Secure Web Portal

Figure **48** is a flowchart of a process **4830** for providing a restaurant supply chain management interface framework. A user is allowed to link to a plurality of restaurant interfaces including information relating to at least one distributor in operation **4832**. One or more distributor links are then displayed on each restaurant interface in operation **4834** with each distributor link capable of linking to a distributor interface including information relating to at least one supplier. At least one supplier link is additionally depicted on each distributor interface in operation **4836** with each supplier link capable of linking to a supplier interface.

In an aspect, all of the interfaces may be written in hypertext mark-up language. In another aspect, the information may identify the distributors and the suppliers. In an additional aspect, the link may include a hyperlink. In a further aspect, the linking may require the entry of an identification code.

Supply Chain Coordinator Web Site/Portal

In an embodiment of the present invention, a supply chain coordinator web site may be provided to allow users easy access to specific information that relates to their role in the restaurant management system.

In one embodiment, users may be registered with the supply chain management system. Upon registration, the user may then be able to access and partake some or all of the features of the supply chain management system. The users can be registered based on information regarding pre-existing relationships, based on new information, etc. Actual registration may be accomplished manually, via telephone, or online for example. Some illustrative registration information that can be collected may include, for example:

- Identification of the user
- User contact information
- User function
- Goods/Service Provider
- Client/Customer
- Billing/Payment Status

The users may be assigned to specific user groups based on their function. Some exemplary user groups include:

- Retail Outlet Members (e.g., Franchisees, Stores, etc.)
- Suppliers
- Distributors
- Retail Outlet Managers
- Retail Outlet Management Corporation
- Supply Chain Coordinator

In addition, users may be linked to the specific retailers, distribution centers and Areas of Direct Influence (ADI's) with which they are involved.

Figure **49** is a schematic illustration of an exemplary supply chain coordinator web site start page **4900** in accordance with an embodiment of the present invention. In a preferred embodiment, the supply chain coordinator web site start page **4900** is accessible via the Internet/World Wide Web. In such an embodiment, any Internet user can get to the supply chain coordinator web site start page. However, preferably, only a user with a valid pre-established user identification can log in to the site. The user identification (user name and password) assigns the user to the appropriate user group and links this user to the appropriate retail outlets, distribution centers and ADI's.

Convenient links to other web sites (e.g., a retail management corporation web site such as, for example, the Burger King Corporation web site, or the National Franchise Association web site) may be included on the supply chain coordinator start page.

In a preferred embodiment, to access the appropriate home page for a specific user group, the user may enter the designated user name **4902** and password **4904** in the log in section near the top of the start page and enters the appropriate site.

Figure **50** is a schematic illustration of an exemplary supply chain coordinator Members' Front Page **5000** in accordance with an embodiment of the present invention. For supply chain coordinator Members, this front page **5000** may be a personalized with the user's name and a timely business reminder **5002** being displayed on the page. A side panel **5004** identifies the user group to which the user belongs and lists those options and reports available to the user. This information may also be displayed in a frame of the page. As illustrated in Figure **50**, some exemplary options/reports that may be displayed in the front page **5000** include:

- Local Promotions **5006** - Contains options specific to those involved with local promotions including adding a new ADI promotion, creating a new promotion and viewing current and historical summary of promotions by ADI
- Franchisee **5008** - Contains options specific to franchisees including the electronic versions of the Red Book and the supply chain coordinator Technology Guide to POS Systems

- Reports **5010** - Allows the user access to a list of reports that provide a wide range of information and enable users to perform their jobs more efficiently.
- Personal Info **5012** - Allows users to maintain their passwords and to view and update their contact information.
- Legal **5014** - Contains details regarding the terms under which supply chain coordinator operates this site and users' obligations in using the site.

Figure **51** is a flowchart of a process **5130** for providing a supplier interface. Utilizing a network, data is received from a plurality of stores of a supply chain in operation **5132**. This data relates to an amount of goods sold by the stores. The data is aggregated in a database in operation **5134**. Subsequently, a request is received from a supplier which includes a plurality of supplier parameters in operation **5136**. Information from the database relevant to the supplier parameters is extracted in response to the request in operation **5138** and the information from the database is transmitted to the supplier utilizing the network in operation **5140**. Also, a supply of raw materials from which the goods are produced is adjusted based on the information in operation **5142**. Note also that the amount/rate of finishing goods and/or supplies can be adjusted based on the information.

In an aspect, the parameters relate to a forecasted amount of the required goods. In another aspect, the network includes the Internet. In a further aspect, the information is displayed utilizing a network-based interface. In one aspect, the stores include restaurants.

Figure **52** is a flowchart of a process **5230** for providing a distributor interface. Data is received from a plurality of stores of a supply chain utilizing a network in operation **5232**. This data relates to an amount of goods sold by the stores and is aggregated in a database in operation **5234**. Upon receiving a request which includes a plurality of distributor parameters from a distributor in operation **5236**, information is extracted in operation **5238** from the database relevant to the distributor parameters in response to the request. The information is then transmitted from the database to the distributor utilizing

the network in operation **5240** and an amount of raw materials purchased in correlation to the production of the goods is adjusted based on the information in operation **5242**.

In an aspect, the parameters relate to a forecasted amount of the required goods to be delivered to the stores. In another aspect, the network includes the Internet. In a further aspect, the information is displayed utilizing a network-based interface. In an additional aspect, the stores include restaurants.

Figure **53** is a schematic illustration of an exemplary POS Implied Daily Usage – Distributor report **5300** that may be displayed in the supply chain coordinator web site in accordance with an embodiment of the present invention. This report provides distribution centers and supply chain coordinator with timely retail outlet sales information, here of a restaurant. This report **5300** uses menu items sales data collected daily from a sample of restaurants served by each distribution center, and recipes for each menu item, to calculate the estimated usage of each inventory item at the distribution center level. In calculating the data, average per restaurant unit sales of each menu item may be computed based on the restaurants sampled and are then multiplied by the total number of restaurants served to determine implied total sales by menu item.

This report **5300** may also include a daily total for each inventory item for the past 14 days and weekly totals for the 4 weeks prior to the 14 days, as well as a calculation of prior day usage as a percentage of average daily usage for the past 14 days. In a preferred embodiment, this report **5300** may be recalculated daily. For example, in an exemplary, a report containing the prior day's sales can be available after 3 PM on the following business day.

Another report that may be displayed via the supply chain coordinator web site is a service level report which lists each distribution center's fill rate, on-time percentage and the percentage of perfect orders. The service level report may also indicate how the fill rate, on-time and perfect order for each distribution center compare to the minimum standards set by supply chain coordinator and restaurant management corporation.

Figure **54** is a schematic illustration of an exemplary local promotion summary – by distribution center report **5400** that may be displayed in the supply chain coordinator web site in accordance with an embodiment of the present invention. This report **5400** provides a summary of all local promotional activity for a distribution center. For each local promotion, the report **5400** may list each participating ADI, the date the promotion started in that ADI, the projected daily sales of the promotional menu item, per restaurant (or other retailer), for the ADI, and how many weeks the promotion will run in that ADI.

The local promotion summary – by distribution center report **5400** may also show how many restaurants in the ADI, which are served by the distribution center, are participating in the promotion, and lists the specific restaurant management company's restaurant numbers for restaurants not participating in the promotion (see "Non-Participating Restaurants" column).

Figure **55** is a schematic illustration of an exemplary POS implied daily usage - supplier report **5500** that may be displayed in the supply chain coordinator web site in accordance with an embodiment of the present invention. This report **5500** provides timely restaurant sales information based on actual restaurant sales to suppliers, supply chain coordinator and supply chain coordinator members. The POS implied daily usage - supplier report **5500** may also use menu item sales data collected daily from a sample of restaurants served by each distribution center, and recipes for each menu item, to calculate the estimated usage of each inventory item provided by the supplier. Usage may be calculated and presented at the distribution center level and totaled by FOB point.

In calculating the data, the average per restaurant unit sales of each menu item are computed based on the restaurants sampled, and then multiplied by the total number of restaurants served to determine implied total sales by menu item. The report **5500** may include:

- a daily total for each inventory item for the past 14 days
- weekly totals for the 4 weeks prior to the 14 days

- a calculation of prior day usage as a percentage of average daily usage for the past 14 days

In a preferred embodiment, the POS implied daily usage - supplier report **5500** may be recalculated daily. For example, a report containing the prior day's sales can be available after 3 PM on the following business day.

Another report that may be displayed via the supply chain coordinator web site is an average restaurant daily POS sales report which provides average restaurant daily menu item sales grouped by category and indicates the changes from a prior period. In a preferred embodiment, this report may be recalculated daily. For example, an average restaurant daily POS sales report containing the prior day's sales can be available after 3 PM on the following business day from the day the information was obtained.

Figure **56** is a schematic illustration of an exemplary restaurant landed cost verification report **5600** that may be displayed in the supply chain coordinator web site in accordance with an embodiment of the present invention. The purpose of the restaurant landed cost verification report **5600** is to inform restaurant operators, for products negotiated by supply chain coordinator, of the contract prices at their back door. In an exemplary embodiment, this report may list:

- the inventory item supplied by the distribution center with the distribution center's cost (see "DC Cost" column)
- the markup amount supply chain coordinator negotiated on behalf of the franchisee (see "Markup" column) and
- the resulting total landed cost as of a specified date (see "Rest Cost" column).

In a preferred embodiment, only inventory items that supply chain coordinator purchases are included. Also, if a franchisee has not appointed supply chain coordinator as supply chain manager, only the distribution center cost will be available in the report and the franchisee may add the mark up as per the franchisee's contract with the distributor. Like the other reports available via the supply chain coordinator web site, the restaurant landed

cost verification report **5600** may be recalculated daily and may be printed at any time for any date.

Figure **57** is a flowchart of a process **5730** for navigating a user in a network-based supply chain management interface. A plurality of stores, distributors and suppliers of a supply chain are registered utilizing the Internet in operation **5732**. Each of the stores, distributors and suppliers is assigned an identifier in operation **5734**. When a request (which includes an identifier) is received from a user for access to a database utilizing a first web-page in operation **5736**, the user is identified as a store, distributor and/or supplier using the identifier in operation **5738**. A second web-page is displayed if the user is identified as a store. A third web-page is displayed if the user is identified as a distributor. A fourth web-page is displayed if the user is identified as a supplier (see operation **5740**).

This provides a degree of confidentiality among competitors who are supply chain participants. Because many of the participants may need to disclose trade secrets to the supply chain manager, such as prices, sources of raw materials, and quantity data, they may be wary of joining. By providing a separate interface on a per-participant basis, trade secretes are protected, and competitors are more likely to join. Further, this avoids antitrust issues, as sales information can be kept secret to all but the supply chain coordinator.

In one aspect, the database may include data representative of sales by the stores. As another aspect, the database may include data representative of goods ordered by the stores. As an additional aspect, the database may include data representative of goods delivered by the distributors. As a further aspect, the database may include data representative of goods in an inventory of the suppliers. Also, the data may be displayed in each of the web-pages utilizing the Internet.

The following sections describe the secure Integrated Supply Chain web portal. The secure web-enabled integrated supply chain portal allows supply chain management to offer supply chain services within a member community.

The sub-sections that follow describe the security process recommendations, policies, functionality, system requirements, user communities, and technical and organizational issues that need to be addressed during the subsequent design, development and implementation phases.

The specifications contained herein express the Integrated Supply Chain web portal preferred Critical-To-Quality (CTQ) factors. One skilled in the art will appreciate that actual implementation of the requirements may differ from that described without straying from the scope of the invention, as the CTQ criteria may evolve and adapt to market conditions or other influences on their strategic vision and direction.

The recommendations include major functional requirements, interfaces, and infrastructure as well as the non-functional requirements (systems and organizational attributes). It includes functional and system needs.

Integrated Supply Chain Web Portal

One goal of the present invention is to enhance Supply Chain management services to improve the efficiency of their member's supply chain.

The underlying concept of electronic commerce (EC) is to use information to displace time and cost in the supply chain. The Integrated Supply Chain Management system (ISCM) portal functions as the electronic commerce facilitator in the supply chain by efficiently collecting, transporting, transforming and sharing information across the enterprise.

Figure **58** depicts a high level view of ISCM communications according to an illustrative embodiment of the present invention. The ISCM **5800** provide two capabilities. The first is to distribute consumption and forecast data to the supply chain participants (franchisees **5802**, distributors **5804**, suppliers **5806**, and raw material suppliers **5808**) that can use it to effective plan purchases and inventory. The second is to automate restaurant ordering (food and packing, equipment and promotions, etc.).

The process works as follows. Restaurants send detailed menu sales information to the ISCM each day from their point of sale (POS) registers. The POS data is converted from menu sales data to material usage data. Specifically a recipe or bill of materials is used to convert each menu item into its purchased components (e.g. bun, meat, wrapper, etc.). The usage data is made available to the supply chain via the ISCM portal. The data is made available to the portal community in the following forms. Distributors see the daily usage of the materials they supply to the restaurants they service. Additionally this usage will be broken down by their distribution center locations. Suppliers see the daily usage of the products/commodities that they supply to the distributors who service the restaurants. Additionally this usage will be broken down by their plant locations. The franchisee and individual restaurants can view sales in the contexts of material usage.

The restaurants can enter orders and send them to the distributor electronically via the ISCM portal. This information enables the entire supply chain to better plan inventory stocking levels and replenishments. This improved planning results in several supply chain efficiencies and benefits. Waste, obsolescence and carrying costs that result from excessive inventories are reduced. The amount of lost sales that result from inventories that are inadequate to meet demand is reduced. Fewer emergency and expedited orders are created. Advanced shipment planning is enabled, which results in lower freight and transportation costs.

The electronic ordering capability enables the restaurants to reduce the costs and times associated with preparing, submitting and receiving orders.

The ISCM system can be enhanced with additional capabilities that serve to further increase the efficiency of the supply chain. These may include electronic invoicing, electronic funds transfer to pay invoices, evaluated receipt settlement, bar coding, and tracking capabilities.

Figure **59** is a flowchart of a process **5930** for tracking the shipment of goods in a network-based supply chain management framework utilizing barcodes. In general, a distributor is sent an order for goods from a supply chain participant utilizing a network in operation **5932**. The goods are then tracked utilizing a bar code in operation **5934**. The results of the tracking are stored in a database in operation **5936** so that the supply chain participant can be allowed to access the results of the tracking utilizing a network with TCP/IP protocol in operation **5938**.

In one aspect of the present invention, the barcode is attached at the start of the process so that a common barcode is used throughout the shipping process. However, barcodes can also be attached at other points in the process if desired.

In an aspect, the network may include the Internet. In another aspect, the results may be accessible utilizing a network-based interface. In a further aspect, the supply chain participant may comprise a restaurant. In one aspect, the supply chain participant may be allowed access only after an identity thereof is verified. In an additional aspect, the goods may have the bar code adhered thereto.

ISCM Access and Security Perspective

System management becomes more complicated when security and access management are added to it. They expand the role of ISCM portal to include the function of enterprise gatekeeper in addition to that of information distribution facilitator.

The underlying concepts of electronic commerce (EC), and security and access management are somewhat at odds. EC makes the supply chain more efficient by

facilitating the flow information throughout the enterprise. Security and access management on the other hand, restricts access and the flow of information. They may be some of the evils that are needed to prevent outsiders from accessing the system and its data, prevent unauthorized users from performing restricted activities, and preserve privacy within the enterprise by limiting data access to a need to know basis.

Although security is an ingredient to the electronic commerce business model, it has a price that can be measured in direct out of pocket costs, ease of use, flexibility, administration overhead, and system maintenance and flexibility. The greater the protection against unauthorized access and use, the greater the cost of the system and the cost of using the system.

Regarding ease of user, the greater the security of a system the harder it is to use. For example, a security arrangement that requires different passwords to access each sub-function of a system would be very secure. On the other hand it would be perceived by its end users as inefficient and hard to use because of the many passwords that are needed. The end users would prefer a less secure single log on that provides them access to all the functions and data in a system.

In an EC community that is populated by several different players, flexibility in specifying access privileges is important. This due to the fact that the access arrangements can accommodate different functions (e.g. franchisees, distributors, suppliers, the supply chain coordinator, retail management, etc.) and different organizations within a given function. The more flexible the system, the easier it is for the users to adapt it to their organization. However, the price of flexibility in this area is either less security (simplicity) or greater complexity and system development and maintenance costs.

The greater the security of a system, the greater the administrative effort needed to setup users and to maintain security. Additionally the administrative effort becomes more

complex as greater security is required and the complexity (effort) increases over time as the system ages.

Complex systems are inflexible and difficult to enhance and maintain. Security makes systems complex in two ways. First, through the introduction of the programs/modules needed to protect the system. Second, by introducing code that attempts to insulate the end user from security (i.e. provide high security without sacrificing flexibility, ease of use, etc.). Insulating complexity can become very pervasive and expensive. As systems grow and expand, the users should be insulated across new modules, features and data views in a fashion consistent with the original approach. This can be difficult when 3rd party software is used or when a new feature does not conform to some earlier assumptions regarding users or system structure.

Security challenges the designers of EC systems to provide a level of security that is appropriate for the system's data and users while minimizing the direct and indirect costs of security that were just discussed. Additionally, the designer may try to anticipate the future growth and the expansion of the EC system so that its security architecture can easily accommodate new features, users and data.

Figure **60** illustrates the ISCM in the context of security and access management. The ISCM System shown in Figure **60** offers several security challenges.

The user community is comprised of several entities. These include retail outlets **6002**, franchisees **6004**, distributors **6006**, suppliers **6008**, the supply chain coordinator **6010** and retailer management **6012**. Security attributes and domains need to be established for each entity. Administrative procedures and programs need to be provided to establish and maintain the security attributes and domains of each of these differing entities.

Security management for data access will be complex because data is shared across the community. A single data item (e.g. daily beef usage for a restaurant) can belong to several domains (e.g. restaurant (retailer), franchisee, distributor, supplier, etc.).

The variety of user communities and the organizational variations that are found within each create a challenge to provide a flexible sub administrative capability that will enable user organizations to manage their own domains.

The security challenges and the tradeoffs created by them will be covered in detail in the technical design and recommendation sections.

User Characteristics

User Relationships

Figure **61** sets forth the members of the ISCM community **6100** and their relationship. From an operational perspective the ISCM community is made up of management members, member retailers, distributors and suppliers. The supply chain coordinator manages the community from both a goods and services and information perspectives.

The community member relationships can be characterized as follows. Supply chain management gives distributors **6102** the exclusive right to supply all retailers **6104** in the distributor's geographic territory. Retailers order from their assigned distributor. Retailer management approves commodity suppliers **6106**. Supply chain management specifies the approved commodity suppliers that each distributor will use. Distributors replenish their inventories by ordering supplies from the suppliers designated by supply chain management.

The purpose of the following sub-sections is to look at the members of the supply chain community in terms of member characteristics (supply chain role that is performed by each member and how each member is organized to perform their role) and members personnel who will likely interact with ISCM. Member domains that will form the basis for security and access management are also defined.

User Organizations

Supply Chain Management

The supply chain coordinator manages the supply chain for their member's retailers. Its services include:

Negotiating supplier agreements on behalf of their members.

Negotiating distributor agreements on behalf of their members. Distributors are given exclusive rights to supply retailers in a given geography. Distributor agreements specify territory, retail outlets, items supplied, suppliers, delivery requirements and quality requirements.

Overseeing and managing the supply chain process to insure consistent and high quality performance.

Providing an ISCM web portal that will make the supply chain more efficient and will enable the members of the supply chain to run their businesses better.

The functions in the following table interact with ISCM:

Table 2

User Function	Description
System administrator	Person who has access to all of the users and capabilities of ISCM. Responsible for creating, modifying and deleting members, distributors and suppliers.
Member administrator	Person who has access to all of the members users of ISCM. Responsible for providing the information for setting up and maintaining members and their domains. Also responsible for providing access to member data to non-member users (e.g.

User Function	Description
	SCC, NFA, RM).
Distributor administrator	Person who has access to all of the distributor users of ISCM. Responsible for providing the information for setting up and maintaining distributors and their domains. Also responsible for providing access to distributor data to non-distributor users (e.g. distributor contract negotiator).
Supplier administrator	Person who has access to all of the supplier users of ISCM. Responsible for providing the information for setting up and maintaining suppliers and their domains. Also responsible for providing access to supplier data to non-supplier users (e.g. supplier contract negotiator).
Operations support / manager	Person has access to system audit log and system operational reports. Responsible identifying things such as attempts to gain unauthorized access, abnormal usage patterns, system bottlenecks, etc.
Help desk	Person(s) responsible for supporting the user community when they have questions or encounter difficulties.

Figure **62** is a flowchart of a process **6230** for selecting suppliers in a supply chain management framework. A network is utilized in operation **6232** to receive data from at least one store of a supply chain that relates to the sale of goods by the at least one store. An electronic order form is generated based on the data for ordering goods from a distributor of the supply chain in operation **6234**. Supplier information is received from a management headquarters utilizing the network in operation **6236**. The supplier information includes a plurality of suppliers selected to supply the store with the goods. The supplier information is then used to transmit the electronic order form to the selected suppliers of the supply chain utilizing the network in operation **6238**.

In one aspect, the network includes the Internet. In another aspect, the electronic order form is generated by the at least one store. In a further aspect, the electronic order form

is generated by the distributor. In an additional aspect, the suppliers are selected using the data. In yet another aspect, the suppliers are selected using performance information collected regarding the suppliers.

Members

The members are franchisees who own one to several hundred retail outlets. They also are the owners of the supply chain coordinator cooperative and as such, they are the primary focus ISCM from efficiency and cost reduction points of view.

In the initial form of ISCM, members perform three functions. They create retailer orders and send them to distributors for processing. They provide daily POS data to supply chain management, who will then enhance it and provide it to members, distributors and supplier on an aggregated basis to assist them in planning inventories and purchases. Also, they retrieve and view orders, and enhanced sales history data.

The member organizations that ISCM can support vary from a single level organization to ones that can contain as many as four levels. The structure depends on the nature of the business entity (sole proprietorship, partnership or corporation), the size (number of retail outlets) and the preferences of the owner/CEO/board/partners. The structure impacts ISCM as it dictates the number (width and depth) of data domain levels that ISCM supports. Figure **63** illustrates a multi-level, complex member organization **6300**. The table below illustrates ISCM user functions. Looking to the Usage Type, an Active User uses ISCM in the course of doing their daily job. A Passive User may use ISCM information; doesn't need it to do job.

Table 3

User Function	Usage Type	Description
Administrator	Active	Responsible for adding, modifying and

User Function	Usage Type	Description
		deleting users in their distributor domain. Sets access permissions for users in their domains.
Corporation/owner/partner: *CEO* *VP of marketing* *VP of development* *CFO* *VP of operations*	Passive	View forecasts, and historical sales and usage for corporate level and sub domains below corporate.
Area staff: *VP* *Director of OPS* *Marketing manager*	Passive	View forecasts, and historical sales and usage for area level and sub domains below area.
District managers	Passive	View forecasts, and historical sales and usage for district level and sub domains below district.
Restaurant managers	Active	View orders, forecasts, and historical sales and usage for restaurant.
Order preparer	Active	View orders, forecasts, and historical sales and usage for restaurant. Enter orders for restaurants.

Distributors

Distributors are middlemen with whom the supply chain coordinator has contracted to supply all member retailers in a given geography.

Distributor supply chain services include:

- Receive, pick, pack and ship retailer orders as specified by the terms and conditions of a supply chain agreement.

- Invoice shipped retailer orders as specified by the terms and conditions of the supply chain agreement.

- Provide warehouse storage space for inventory levels that are sufficient to service the retailers in their geography as specified by the terms and conditions of the supply chain agreement.

- Provide storage environments (e.g. refrigeration) that are needed to maintain the quality of the items they supply to the retailers in their geography.

- Maintain inventory levels that are sufficient to supply retailers as specified by the terms and conditions of the supply chain agreement.

- Replenish inventories by buying from approved and/or pre-specified suppliers.

The distributors serve a large geography. As a result, they have several strategically located distribution centers throughout their territory. These distribution centers maintain local inventories and service retailers in their locale to reduce transportation time and costs.

Functions such as sales, accounting, billing, customer service, are generally centralized at a headquarters location.

The supply chain coordinator's contracts with distributors specify:

- Service levels that cover things like order cycle times, commodity quality, etc.
- Retailers served by the distributor.
- Distribution center that services each retailer.

- Items/commodities that the distributors will carry in their inventory for the retailers.
- Suppliers and supplier plant that will be used to provide each item that will be carried by each distribution center for the retailers they service.

Figure **64** is a flowchart of a process **6430** for contract enforcement in a supply chain management framework in which data is collected from a plurality of stores of a supply chain utilizing a network in operation **6432**. Next, a network-based interface is displayed for allowing access to the data in operation **6434**. An electronic order form is then generated in operation **6436** based on the data utilizing the network-based interface for ordering goods from a distributor of the supply chain, the electronic order including a contact with terms of a delivery of the goods. Information relating to the delivery and/or costs of the goods is tracked utilizing the network in operation **6438** and the tracked information is compared with the terms of the contract in operation **6440**.

In one aspect, the information relates to a timeliness of delivery of the goods. In another aspect, the information relates to a quality of the goods delivered by the distributor. In a further aspect, the information relates to a price of the goods delivered by the distributor. In an additional aspect, an alert is sent upon the comparison indicating a discrepancy between the tracked information and the terms of the contract. In such an aspect, the alert may be made available on the network-based interface.

The following table lists distributor functions that may interact with ISCM:

Table 4

User Function	Usage Type	Description
Administrator	Active	Responsible for adding, modifying and deleting users in their distributor domain. Sets access permissions for users in their domains.

User Function	Usage Type	Description
Headquarters: CEO/GM Marketing Procurement Credit Accounts receivable Accounts payable	Passive	View orders, forecasts, and historical sales and usage for corporate level and distribution centers below corporate level.
Customer Service QA	Active	View orders for all distribution centers to deal with retailers question/issues
Account executive	Active	Distributor point of contact for the supply chain coordinator. View orders, forecasts, and historical sales and usage for corporate level and distribution centers below corporate level.
Contract manager	Active	View orders, forecasts, and historical sales and usage for corporate level and distribution centers below corporate level.
Distribution Center: DC buyer	Active	View forecasts, and historical sales and usage by supplier for DC. Uses information to plan purchases
Transportation manager	Active	View orders and forecasts to schedule trucks and determine routes.
Order pickers	Active	View individual orders to pick them
Shipping	Active	View individual orders to pack and ship them.

Usage Type: Active User uses ISCM in the course of doing their daily job.

Passive User may use ISCM information; doesn't need it to do job.

Figure **65** is a flowchart of a process **6530** for monitoring distributor activity in a supply chain management framework. Data is received in operation **6532** from at least one store of a supply chain utilizing a network. This data relates to the sale of goods by the store. Electronic order forms are generated in operation **6534** based on the data for ordering goods from a plurality of distributors of the supply chain. The generated electronic order forms are sent to the distributors in operation **6536** so that the goods are delivered to the stores. The electronic order forms for each of the distributors are compared for monitoring the reliance of the store on each distributor in operation **6538**.

In one aspect, the network includes the Internet. In another aspect, the electronic order forms are generated by the at least one store. In a further aspect, the comparison is accessible utilizing a network-based interface. In an additional aspect, the electronic order forms indicate a type of the goods, an amount of goods, and a target delivery date of the goods. In another aspect, the comparison is used to gauge a performance of the distributors.

<u>Suppliers</u>

Suppliers produce the items that the retailers buy from the distributors. Distributors replenish their inventories with bulk purchases from suppliers.

All suppliers are approved by retail outlet management. The supply chain coordinator negotiates agreements with suppliers on behalf of their members. Distributors can utilize supply chain coordinator-specified suppliers to service the restraints.

Large national/regional suppliers will have several production/processing facilities around the country. The facilities that will supply the distributors are inspected and approved by retailer management. The supply chain coordinator can specify the supplier facility that will be used to replenish each distributor distribution center.

The following table has supplier functions that may interact with ISCM:

Table 5

User Function	Usage Type	Description
Administrator	Active	Responsible for adding, modifying and deleting users in their supplier domain. Sets access permissions for users in their domains.
Headquarters: Marketing Procurement Credit Accounts receivable Accounts payable	Passive	View item forecasts and historical sales and usage for corporate level and for plants below corporate level.
Account executive	Active	Supplier point of contact for the supply chain coordinator. View item forecasts and historical sales and usage for corporate level and for plants below corporate level.
Plant: Production planner		View item forecasts, and historical sales and usage. Use to plan production.
Buyer	Active	View item forecasts, and historical sales and usage. Use to plan production material purchasing.
Transportation manager	Active	View item forecasts, and historical sales and usage. Use to plan transportation.

Usage Type: Active User uses ISCM in the course of doing their daily job.

Passive User may use ISCM information; doesn't need it to do job.

Figure **66** is a flowchart of a process **6630** for monitoring supplier activity in a supply chain management framework. Data relating to the sale of goods is received from at least one store of a supply chain utilizing a network in operation **6632**. Electronic order forms

are generated based on the data for ordering goods from a plurality of suppliers of the supply chain in operation **6634**. The electronic order forms are sent to the suppliers so that the goods are supplied to the stores in operation **6636**. The electronic order forms for each of the suppliers are then compared for monitoring the reliance of the store on each supplier in operation **6638**.

In one aspect, the network includes the Internet. In another aspect, the electronic order forms are generated by the at least one store. In a further aspect, the comparison is accessible utilizing a network-based interface. In yet another aspect, the electronic order forms indicate a type of the goods and an amount of goods. In an additional aspect, the comparison is used to gauge a performance of the suppliers.

User Relationship Domains for Access and Reporting

The following table depicts the domains for access and reporting for members, distributors and suppliers.

Table 6

Member	Member Area District Retailer Item Quantity
Distributor	Distributor (order) Distribution center Retailer Item Quantity Distributor (usage)

	Item Distribution center Supplier Supplier plant Item Quantity
Supplier	Supplier Plant Item Quantity

Figure **67** is a flowchart of a process **6730** for a bulletin board feature in a supply chain management framework. Utilizing a network, data is collected from a plurality of stores of a supply chain in operation **6732**. A network-based interface is also displayed for allowing access to the data in operation **6734**. An electronic order form is generated in operation **6736** based on the data utilizing the network-based interface for ordering goods from selected distributors of the supply chain. The network-based interface includes a bulletin board displaying information received from each of the stores. The received information relates to the distributors for facilitating the selection of the distributors.

In one aspect, the information relates to a timeliness of deliveries made by the distributors. In another aspect, the information relates to a quality of the goods delivered by the distributors. In a further aspect, the information relates to a price of the goods delivered by the distributors. In an additional aspect, a store from which the information is received is identified. As another aspect, the store from which the information is received may be identified utilizing an electronic mail address for communication purposes.

Figure **68** is a flowchart of a process **6830** for a catalog feature in a supply chain management framework. Data is collected utilizing a network in operation **6832** from a plurality of stores of a supply chain. A network-based interface is displayed in operation

6834 for allowing access to the data. An electronic order form is subsequently generated in operation **6836** based on the data utilizing the network-based interface for ordering goods from a distributor of the supply chain or a supplier of the supply chain if the goods are not distributed through a distributor. The network-based interface includes a virtual catalog to facilitate the generation of the electronic order form.

In an aspect, the catalog displays a plurality of raw products from which the goods are produced. In such an aspect, the catalog may display a plurality of distributors from which the raw products can be ordered. As a further aspect, the catalog may also display a comparison of performance of the distributors. As an additional aspect, the performance may be calculated based on the data. In an another aspect, the catalog may include links to additional network-based interfaces relating to suppliers.

Critical To Quality Requirements

Overview

When defining the features and functionality of a newly designed system, it is recommended to begin with the actual business needs of the users of the web portal. It has already been defined in the section entitled **User Characteristics** that the users of the web portal will be managing and maintaining many if not all of the security administrative aspects of the system.

It is important to gather and understand the business needs for each user community and then translate those needs into actual Critical To Quality (CTQ) requirements. To obtain these CTQs, each user group supplied their own Voice Of the Customer (VOC) demands upon the system.

The VOCs are then mapped into high level categories that ultimately map to desired features and functional requirements (discussed in the section entitled **Functional Requirements**, below).

The overall approach uses a six sigma consulting methodology **6900** for mapping customers directly to solution design and is outlined in the Figure **69**.

Using this approach, it is possible to design a system solution that ties directly back to the core customer groups and their business needs. Features and high level functional requirements are the core to system design, and using the Six Sigma consulting methodology maintains the integrity of the original business needs as presented by the key stakeholders for the web portal.

The next set of sections will detail the specific VOCs and CTQs that were collected in the workshop sessions. These CTQs will then be tied to the features and functional requirements as outlined in the section entitled **Functional Requirements**, below.

Voice Of the Customer (VOC)

Each of the core customer communities as outlined in the section entitled **User Characteristics** were interviewed to collect their VOCs in relation to a web security model. Each workshop discussed potential portal applications and their functionality, providing a back drop for the potential security needs of the system. The following table lists all of the VOCs collected at each workshop, and places them into high level categories.

Table 7

	Voice of the Customer	SCC	Member	Supplier Distributor
1.	Securely isolate data and functions to prevent unauthorized access.			
	Isolate my data	X		
	My data for my eyes only	X		

	Voice of the Customer	SCC	Member	Supplier Distributor
	Insure my data is safe	X		
	Want to feel the system is secure		X	
	Assume a high level of security; keep competitors out		X	X
	Ability to perform password administration and manage accounts	X	X	X
	Access right/password changes must be granted immediately.		X	
	System should require periodic password changes for all accounts			X
	Make it difficult for someone to take data directly to a competitor			X
2.	Security is simple from an end user's perspective.			
	Make it quick and easy	X		
	Give me a single logon with multiple community access.	X	X	
	Ability to select access rights for all levels		X	
	If you make it too difficult to access we won't want to bother accessing it.			X
3.	Security administration is simple from a user perspective			
	Make maintenance simple		X	
4.	Access management administration is very flexible.			
	Give me a single logon with multiple community access.	X	X	
	Ability to select access rights for all levels		X	

	Voice of the Customer	SCC	Member	Supplier Distributor
	Simultaneous/reciprocal access		X	
	Be able to select individuals to set up access to his/her group			X
	Various levels would have varying degrees of password change enforcement			X
	We need multiple levels of security access			X
	Single individuals may have multiple owner organizations			X
	I need flexibility			X
5.	System proactively monitors for potential security breaches.			
	I want the system to take preventative measures		X	
	We should be able to detect that something isn't right		X	
	We want an audit trail of some sort			X
	Incident tracking capability; especially for inappropriate use.			X
6.	Reports are available that enable community administrator to effectively manage and maintain security and access.			
	Tell me who is using the SCC web site	X		
	Show me who is using the system for my organization	X		
	Who has done what to my data?		X	
	I want reporting functionality for audits.		X	
	We should be able to detect that something isn't right		X	

	Voice of the Customer	SCC	Member	Supplier Distributor
	We want an audit trail of some sort			X
	Want to track information flow			X
	Need to know who has access			X
	Need to have detailed information available to determine who went where when.			X
	Incident tracking capability; especially for inappropriate use.			X
7.	System does not create cost or incremental effort for the supply chain community			
	Don't waste time on the Internet	X		
	No incremental cost	X	X	X
	Don't disrupt my business operations		X	
	I don't want to hire anyone for support or administration		X	
	I'm concerned about information overload			X
	Target the information and give me what I need to know.			X
	This is supposed to represent cost savings			X
8.	Effective training and documentation			
	Create a common nomenclature (classification and roles)			X
	Training concerns			X
9.	Integrate with existing systems			
	Single sign-on	X	X	
	One location "one-stop-shop"		X	

CTQs

The VOCs identify most of the security concerns for each user community. These statements are then assessed to fall into distinct and measurable requirements, the critical to quality factors for each of the stated issues.

The following table outlines how each of the high level VOCs categories map to specific CTQ requirements and these items will ultimately map to the desired features and functionality of the security system.

Table 8

	Voice of the Customer	CTQ
1.	Securely isolate data and functions to prevent unauthorized access.	Security, Prevention
2.	Security is simple from an end user's perspective.	Simplicity
3.	Security administration is simple from a user perspective	Simplicity, Ease of Use
4.	Access management administration is very flexible.	Flexibility
5.	System proactively monitors for potential security breaches.	Reporting, Prevention
6.	Reports are available that enable community administrator to effectively manage and maintain security and access.	Reporting, Simplicity, Prevention
7.	System does not create cost or incremental effort for the supply chain community	Cost
8.	Effective training and documentation	Simplicity
9.	Integrate with existing systems	Integration,

	Voice of the Customer	CTQ
		Simplicity

Business Processes

Overview

Any security model will require certain business processes and procedures to maintain the integrity and ease of use. This section outlines some business processes that need to be in place to begin implementation.

The next section, entitled **Policy Requirements**, will further identify specify policies that surround and govern aspects of these processes. It is important to note that these procedures need to be assigned clearly to responsible parties, and the policies outlined in the Section entitled **Policy Requirements** (below) should be clearly provided in order to maintain system integrity.

Adding and Deleting Users

The first procedure that needs to be addressed is how to add and delete users to the system. Users are defined as an individual who requires access to applications and data on the web portal. This process should be replicated throughout the domains and user communities, always managed by a specifically named administrator role (see Administration below).

Adding New Users

The sequence of steps for adding a user begins with authorization:

1. Request for new user account
2. Request verified by administrator, notification sent to user's manager
3. Authorization of new account provided
4. Reference to policy for access rights and privileges for the requested class of user
5. Configure access levels
6. Send new user ID and default password to new user
7. Confirm successful logon and password change at first logon

These steps can exist at all user community levels, and also for providing administrator access, such as from the supply chain coordinator corporate to a Member organization. It is important to provide an authorization step before creating an account, so that the administrator is also monitored for security purposes.

Deleting Existing Users

The sequence of steps for deleting a user requires similar authorization:

1. Request for deleting an existing account
2. Request verified by administrator, notification sent to user's manager
3. Authorization for deleting account provided
4. Reference to policy for deleting access rights and privileges for the requested class of user
5. Delete user account
6. Send verification of deletion to user's manager
7. Confirm successful deletion by attempting administrator logon

The confirmation of deletion may be a useful step, as security breaches are most likely to occur from an improperly deleted account. The supply chain coordinator should require all levels of security management to provide verification of deleted accounts, especially in the member and supplier/distributor communities.

Changing Key Contact Administrator

At times the key contact administrator within a domain organization may change. While the process of adding a new user as an administrator follows the same process as adding a new user, there are a few additional kick-off steps that initiate the process. The key contact in this process is not the account contact (not the Member owner, or supplier contact person), but is in fact the web portal administrator for that organization.

1. Supplier/Distributor/Member notifies the supply chain coordinator account manager of change in key contact.
2. The account manager validates change via phone call to Supplier/Distributor/Member
3. Upon verification, the account manager notifies the supply chain coordinator administrator of new key contact information
4. The administrator suspends user account rights and privileges
5. The administrator sets up new user account with organization administration rights according to access policy guidelines
6. Notify new administrator of new user ID and default password
7. Confirm successful logon and password change at first logon

When the key contact for the security system changes at a domain organization, it is not likely that the supply chain coordinator administrator will be directly notified of the change. That is why it is useful for the account manager to verify the change, and obtain the new user information and submit the request. This process ensures that the administrator is acting upon an authorized and verified request. The process may be audited to trace where the authorization initiated, in the event a false transfer of rights is made.

Auditing and Monitoring

This section describes in detail the procedures to follow for auditing and monitoring the security system usage. What to collect, how to collect it, and how to preserve the integrity of the audit data are all useful procedures for maintaining proper and effective security measures.

Data to Collect

Figure **70** is a flowchart of a process **7030** for electronic invoice auditing in a supply chain management framework. Utilizing a network, data is collected in operation **7032** from a plurality of stores of a supply chain that relates to the sale of goods by the stores. Access to the data is allowed utilizing a network-based interface in operation **7034**. Electronic order forms are generated in operation **7036** based on the data for ordering goods from a plurality of distributors of the supply chain. The generated electronic order forms are sent to the distributors utilizing the network in operation **7038**. Subsequently, invoices are received from the distributors utilizing the network in operation **7040** and the invoices are compared with the electronic order forms for auditing the invoices in operation **7042**.

In one aspect, the electronic order forms include a price of the goods. In another aspect, a price of the goods is calculated from the electronic order forms. In such an aspect, the price of the goods may be calculated from the electronic order forms utilizing a table mapping a plurality of goods with a plurality of prices. In further aspect, the electronic order forms are generated by the stores. In an additional aspect, an alert is generated upon a discrepancy being found during the comparison.

Audit data should include any attempt to achieve a different security level by any person, process, or other entity in the network. This information includes login and logout, super user access (administrator rights), and any other change of access or status. The processes outlined previously include a fair amount of authorization and verification steps—these steps are important to create cross domain, cross organizational audit trails.

The actual data to collect may differ for the different types of applications and different types of access changes made within the portal. In general, the information to collect includes:

- Username, for login and logouts
- Previous and new access rights, to track changes to access
- Timestamp

One very important note: Do not gather passwords. There is an enormous potential for security breach if the audit records are improperly accessed. Do not gather incorrect passwords either, as they often differ from the correct passwords by only a single character or transposition.

Collection Process

There are basically three ways to store audit records:

1. Read / write file on a host
2. Write-once / read-many device (CD-ROM or tape drive)
3. Write-only device (e.g. line printer)

File system logging is also the least reliable method. If the logging host has been compromised, the file system is usually the first thing to go—and an intruder could easily cover up traces of the intrusion.

Collecting audit data on a write-once device is slightly more effort to configure than a simple file, but it has the significant advantage of greatly increased security because an intruder could not alter the data showing that an intrusion has occurred. The disadvantage of this method is the need to maintain a supply of storage media and the cost of that media. Also, the data may not be instantly available.

Line printer logging is useful in system where permanent and immediate logs are required. A real time system is an example of this, where the exact point of a failure or attack may be recorded. A laser printer, or other device that buffers data (e.g., a print server), may suffer from lost data if buffers contain the needed data at a critical instant. The disadvantage of, literally, "paper trails" is the need to keep the printer fed and the need to scan records by hand. There is also the issue of where to store the, potentially, enormous volume of paper that may be generated.

For each of the logging methods described, there is also the issue of securing the path between the device generating the log and actual logging device (i.e., the file server, tape/CD-ROM drive, printer). If that path is compromised, logging can be stopped. In an ideal world, the logging device would be directly attached by a single, simple, point-to-point cable. Since that is usually impractical, the path may pass through the minimum number of networks and routers.

If the supply chain coordinator selects an outsourced host for the security system, these options can be optimized against security breaches. Keeping this audit collection process in-house would require effort to secure the various options for maintaining audit data integrity, detailed further in the following sub-section.

Preserving Audit Data

Audit data should be some of the most carefully secured data at the site and in the backups. If an intruder were to gain access to audit logs, the systems themselves, in addition to the data would be at risk.

Audit data may also become useful to the investigation, apprehension, and prosecution of the perpetrator of an incident. If a data handling plan is not adequately defined prior to an incident, it may mean that there is no recourse in the aftermath of an event, and it may create liability resulting from improper treatment of the data.

Legal Considerations

Due to the content of audit data, there are a number of legal questions that arise which might need to be addressed by legal counsel. As the Supply Chain management system collects and saves audit data, it needs to be prepared for consequences resulting both from its existence and its content.

One area concerns the privacy of individuals. In certain instances, audit data may contain personal information. Searching through the data, even for a routine check of the system's security, could represent an invasion of privacy. The privacy policy outlined in the **Policy Requirements** section (below) should clearly outline procedures that guarantee privacy of an individual user, both in terms of existing contracts (such as between members and retailer management) and also other existing legal regulations.

A second area of concern involves knowledge of intrusive behavior originating from the web portal. If an organization keeps audit data, is it responsible for examining it to search for incidents? If a host in one organization is used as a launching point for an attack against another organization, can the second organization use the audit data of the first organization to prove negligence on the part of that organization?

Security Incident Handling

The operative philosophy in the event of a breach of web security is to react according to a plan. This is true whether the breach is the result of an external intruder attack, unintentional damage, a student testing some new program to exploit vulnerability, or a disgruntled employee. Each of the possible types of events, such as those just listed, should be addressed in advance by adequate contingency plans.

Traditional web security, while quite important in the overall site security plan, usually pays little attention to how to actually handle an attack once one occurs. When an attack is in progress, many decisions are made in haste and can be damaging while tracking

down the source of the incident, collecting evidence to be used in prosecution efforts, preparing for the recovery of the system, and protecting the valuable data contained on the system.

One of the most important, and often overlooked, benefits for efficient incident handling is an economic one. Having both technical and managerial personnel respond to an incident requires considerable resources. If trained to handle incidents efficiently, less staff time is required when one occurs.

Another benefit is related to public relations. News about computer security incidents tends to be damaging to an organization's stature among current or potential clients. Efficient incident handling minimizes the potential for negative exposure. In the member community it is important to maintain good public relations with retail management, suppliers, and distributors in the interest of positive supply chain collaboration.

A final benefit of efficient incident handling is related to legal issues. It is possible that in the near future organizations may be held responsible because one of their nodes was used to launch a network attack. In a similar vein, people who develop patches or workarounds may be sued if the patches or workarounds are ineffective, resulting in compromise of the systems, or, if the patches or workarounds themselves damage systems. Knowing about operating system vulnerabilities and patterns of attacks, and then taking appropriate measures to counter these potential threats may be helpful in circumventing possible legal problems.

This section will outline and discuss the following areas of incident handling:

- Notification
- Identifying an Incident
- Law Enforcement and Legislative Agencies
- Internal and External Communications
- Containment

- On-going Activities

Notification

It is important to establish contacts with various personnel before a real incident occurs. These contacts should include local managers and system administrators, administrative contacts for other domain organizations, and various investigative organizations.

For each type of communication contact, specific "Points of Contact" (POC) should be defined. These may be technical or administrative in nature and may include legal or investigative agencies as well as service providers and vendors. When establishing these contacts, it is important to decide how much information will be shared with each class of contact. It is especially important to define, ahead of time, what information will be shared with the users at a site, with the public (including the press), and with other sites.

A list of contacts in each of these categories is an important time saver for the key contact individuals during an incident. It can be quite difficult to find an appropriate person during an incident when many urgent events are ongoing. It is strongly recommended that all relevant telephone numbers (also electronic mail addresses and fax numbers) be included in the site security policy. The names and contact information of all individuals who will be directly involved in the handling of an incident should be placed at the top of this list.

Identifying an Incident

When an incident occurs, the first step is to identify if it truly is a security incident. Most signs of virus infection, system intrusions, malicious users, etc., are simply anomalies such as hardware failures or suspicious system/user behavior. To assist in identifying whether there really is an incident, it is usually helpful to obtain and use any detection software that may be available. Audit information is also extremely useful, especially in determining whether there is a network attack.

It is extremely important to obtain a system snapshot as soon as one suspects that something is wrong. Many incidents cause a dynamic chain of events to occur, and an initial system snapshot may be the most valuable tool for identifying the problem and any source of attack. Finally, it is important to start a log book. Recording system events, access to data, time stamps, etc., may lead to a more rapid and systematic identification of the problem, and is the basis for subsequent stages of incident handling.

There are certain indications or "symptoms" of an incident that deserve special attention:

1. System crashes.
2. New user accounts (unusual or non-precedent nomenclature, or high activity on a previously low usage account)
3. New files created (usually with strange file names, such as data.xx or *.xx).
4. Accounting discrepancies
5. Changes in file lengths or dates without proper authorization
6. Attempts to write to system without authorization
7. Data modification or deletion (complaints that files or data start to disappear)
8. Denial of service
9. Unexplained, poor system performance
10. Anomalies (e.g. frequent and unexplained "beeps").
11. Suspicious probes (there are numerous unsuccessful login attempts)
12. Suspicious browsing (someone accesses file after file on many user accounts.)
13. Inability of a user to log in due to modifications of his/her account.

This list is not comprehensive, but does highlight some common indicators of security incidents. It is recommended to collaborate with other technical and web security personnel to make a decision as a group about whether an incident is occurring.

Law Enforcement and Investigative Agencies

In the event of an incident with legal consequences, it is important to establish contact with investigative agencies (e.g., the FBI and Secret Service in the U.S.) as soon as possible. It should be acknowledged that the supply chain coordinator and it's user community organizations may have its own local and governmental laws and regulations that will impact how they interact with law enforcement and investigative agencies. The security policies and procedures need to identify those potential differences to help the various domain organizations follow consistent incident response methods.

The supply chain coordinator should notify legal counsel soon after knowledge of an incident is in progress. At a minimum, legal counsel needs to be involved to protect the legal and financial interests of the web portal and subsequent member organizations. There are many legal and practical issues, a few of which are:

1. Negative publicity—Is the supply chain coordinator willing to risk negative publicity or exposure to cooperate with legal prosecution efforts.
2. Downstream liability—Leaving a compromised system as is so it can be monitored while allowing access that causes damage on a downstream system may force liability on the supply chain coordinator for damages incurred.
3. Distribution of information—If the supply chain coordinator web portal distributes information about an attack in which another site or organization may be involved or the vulnerability in a product that may affect ability to market that product, the supply chain coordinator may again be liable for any damages (including damage of reputation).
4. Liabilities due to monitoring— the supply chain coordinator may be sued if users at its site or elsewhere discover that the web portal is monitoring account activity without informing users.

There are no clear precedents yet on the liabilities or responsibilities of organizations involved in a security incident or who might be involved in supporting an investigative effort. Investigators will often encourage organizations to help trace and monitor intruders. Indeed, most investigators cannot pursue computer intrusions without extensive

support from the organizations involved. However, investigators cannot provide protection from liability claims, and these kinds of efforts may drag on for months and may take a lot of effort.

On the other hand, an organization's legal council may advise extreme caution and suggest that tracing activities be halted and an intruder shut out of the system. This, in itself, may not provide protection from liability, and may prevent investigators from identifying the perpetrator.

The balance between supporting investigative activity and limiting liability is tricky. the supply chain coordinator should consider the advice of legal counsel and the damage the intruder is causing (if any) when making the decision about what to do during any particular incident.

Internal and External Communications

It is crucial during a major incident to communicate why certain actions are being taken, and how the users (or departments) are expected to behave. In particular, it should be made very clear to users what they are allowed to say (and not say) to the outside world (including other departments). For example, it would not be good for an organization if users replied to customers with something like, "I'm sorry the systems are down, we've had an intruder and we are trying to clean things up." It would be much better if they were instructed to respond with a prepared statement like, "I'm sorry our systems are unavailable, they are being maintained for better service in the future."

Communications with customers and contract partners should be handled in a sensible, but sensitive way. One can prepare for the main issues by preparing a checklist. When an incident occurs, the checklist can be used with the addition of a sentence or two for the specific circumstances of the incident.

One of the most important issues to consider is when, who, and how much to release to the general public through the press. The public relations office is trained in the type and wording of information released, and will help to assure that the image of the site is protected during and after the incident (if possible). A public relations office has the advantage that one can communicate candidly with them, and provide a buffer between the constant press attention and the need of the POC to maintain control over the incident.

If a public relations office is not available, the information released to the press can be carefully considered. If the information is sensitive, it may be advantageous to provide only minimal or overview information to the press. It is possible that any information provided to the press will be quickly reviewed by the perpetrator of the incident. Also note that misleading the press may backfire and cause more damage than releasing sensitive information.

Some guidelines to keep in mind are:

1. Provide low levels of technical detail.
   Detailed information about the incident may provide enough information for others to launch similar attacks on other sites, or even damage the site's ability to prosecute the guilty party once the event is over.

2. Do not speculate.
   Speculation of who is causing the incident or the motives are very likely to be in error and may cause an inflamed view of the incident.

3. Cooperate with law enforcement.
   Work with law enforcement professionals to assure that evidence is protected. If prosecution is involved, assure that the evidence collected is not divulged to the press.

4. Maintain focus on containment and recovery.

   Do not allow the press attention to detract from the handling of the event. It is of primary importance to contain the incident and begin recovery efforts.

Containment

The purpose of containment is to limit the extent of an attack. A part of containment is decision making (e.g., determining whether to shut a system down, disconnect from a network, monitor system or network activity, set traps, disable functions such as remote file transfer, etc.).

Sometimes this decision is trivial; shut the system down if the information is classified, sensitive, or proprietary. Removing all access while an incident is in progress obviously notifies all users, including the alleged problem users, that the administrators are aware of a problem; this may have a deleterious effect on an investigation. In some cases, it is prudent to remove all access or functionality as soon as possible, then restore normal operation in limited stages. In other cases, it is worthwhile to risk some damage to the system if keeping the system up might enable identification of an intruder.

The supply chain coordinator should define acceptable risks in dealing with an incident, and should prescribe specific actions and strategies accordingly. If features and functionality need to be shut town temporarily, there should be a notification process as well as a back-up (non-web based) process to continue normal business operations. As application functionality is implemented into the web portal, each web feature needs to address the potential for shutdown.

On-going Activities

There are a number of steps the supply chain coordinator should implement to keep up with changes in web security. The following is a list of activities to include for continual incident tracking and handling measures:

1. Subscribe to advisories that are issued by various security incident response teams, like those of the CERT Coordination Center, and update systems against those threats that apply to the supply chain coordinator's web portal technology.

2. Monitor security patches that are produced by the vendors of equipment, software, applications, and third party affiliates, and obtain and install all that apply.

3. Actively watch the configurations of the supply chain coordinator systems to identify any changes that may have occurred, and investigate all anomalies.

4. Review all security policies and procedures annually (at a minimum).

5. Regularly check for compliance with policies and procedures. This audit should be performed by someone other than the people who define or implement the policies and procedures.

Policy Requirements

Overview

Web Portal security policies are designed to address security issues within an Internet community. The supply chain coordinator needs a guide to setting computer security policies and procedures for sites that have systems on the Internet—and may need to also address sites and systems that are not yet connected to the Internet.

The web portal team will need to make many decisions, gain agreement and then communicate and implement these security policies. The focus of this section is on the

policies and procedures that need to be in place in order to support the technical security features of the ISC web portal.

The basic approach to developing a security policy plan for a web portal follows traditional protection rules for overall system security [Fites, 1989 Control and Security of Computer Information Systems]:

1. Identify what you are trying to protect
2. Determine what you are trying to protect it from
3. Determine how likely the threats are
4. Implement measures which will protect your assets in a cost-effective manner
5. Review the process continuously; make improvements each time a weakness is found

Using approach, the supply chain coordinator will be able to continually identify critical assets and required policies throughout the implementation phase for both the security system, as well as future releases of functionality for the web portal.

Setting Goals for A Security Policy

The types of security-related decisions that are made, or the failure to make them, largely determine how secure or insecure the web portal will be, how much functionality the portal will offer, and how easy the portal is to use. To effectively use security tools and policies, the supply chain coordinator may determine its security goals clearly.

Trade-offs exist when defining goals, as outlined here:

- Services Offered vs. Security Provided
  Each service offered to users carries its own security risks. For some services the risk outweighs the benefit of the service, and the administrator may choose to eliminate the service, rather than try to secure it.

- Ease of Use vs. Security

  The easiest system to use would allow access to any user and require no passwords; that is, there would be no security. Requiring passwords makes the system a little less convenient, but more secure. Requiring device-generated one-time passwords (e.g. secure id tokens), makes the system even more difficult to use, but much more secure.

- Cost of Security vs. Risk of Loss

  There are many different costs to security: Monetary, Performance, and Ease of Use. There are also many levels of risk: Loss of Privacy, Loss of Data, and Loss of Service. Each type of cost can be weighed against each type of loss for optimization.

the supply chain coordinator goals should be communicated to all users, operations staff, and managers through a set of security rules, called a "security policy." The scope of this policy includes all types of information technology as well as the information stored and manipulated by the technology.

Purpose of A Security Policy

The main purpose of a security policy is to inform users, staff and managers of their obligatory requirements for protecting technology and information assets. The policy should specify the mechanisms through with these requirements may be met. Another purpose is to provide a baseline from which to acquire, configure and audit systems and networks for compliance with the policy. Therefore an attempt to use a set of security tools in the absence of at least an implied security policy is meaningless.

Assets and Threats

The cost of protecting oneself against a threat should be less than the cost of recovering if the threat were to strike. Cost in this context should include losses expressed in real currency, reputation, and trustworthiness. Without reasonable knowledge of what one is protecting and what the likely threats are, following this rule of cost-effectiveness may be difficult.

It is recommended that as the supply chain coordinator designs and implements additional functionality to their ISC web portal, they examine the extent of security levels and features in relation to the value of the assets involved. There are two elements of risk analysis that one should consider:

1. Identifying the assets
2. Identifying the threats

Identifying the Assets

Figure **71** is a flowchart of a process **7130** for providing a network-based supply chain interface capable of maintaining the anonymity of supply chain participants in the supply chain. Data is received via a network from a plurality of supply chain participants of a supply chain in operation **7132**. Each of the supply chain participants is assigned with an identifier in operation **7134** and the data for each of the supply chain participants is listed utilizing the identifier to preserve the anonymity of the supply chain participants in operation **7136**.

In an aspect, the network may include the Internet. In another aspect, the identifier may include a numeric string. In a further aspect, the identifier may indicate a region where the associated store is located. In an additional aspect, the data may be listed utilizing a network-based interface. In one aspect, the supply chain participants may include restaurants.

For each asset, the basic goals of security are availability, confidentiality, and integrity. Each threat should be examined considering how it may affect these areas. The first step for asset protection is to identify all of the things that need protection. The point is to list all things that could be affected by a security problem. Again, a traditional list for system protection is applicable in the Internet arena:

- Hardware: boards, keyboards, workstations, personal computers, printers, communication lines, servers, routers
- Software: source programs, object programs, utilities, diagnostic programs, operating systems, communication programs
- Data: during execution, stored on-line, archived off-line, backups, audit logs, databases, in transit over communication media
- People: users, administrators, hardware maintainers
- Documentation: on programs, hardware, systems, local administrative procedures
- Supplies: paper, forms, ribbons, magnetic media

The supply chain coordinator should use the preliminary goals and objectives for the ISC web portal to identify the primary assets. Existing procedures and policies for system protection is a good starting point to begin the process for asset identification.

Once identified, it is important to note the differing levels of importance for each of these categories to the users of the portal. For example, a member may hold his or her hardware assets at a higher protection value than a supplier, who may have leased assets or complete warranty and maintenance coverage. Documentation for procedures may have higher value for the administrators at the supply chain coordinator corporate, and

less so at an end user level, as reliance on the accuracy of these materials falls into a very defined set of users.

Identifying the Threats

Once the assets requiring protection are identified, it may be useful to identify the threats to those assets. The threats may then be examined to determine what potential for loss exists. The following are classic threats to be considered:

1. Unauthorized access to resources and/or information
2. Unintended and/or unauthorized disclosure of information
3. Denial of service

The remainder of this section will outline and identify security policies that address these types of threats for most types of assets.

Creating Policy

In order for a security policy to be appropriate and effective, it needs to have the acceptance and support of all levels of employees within an organization. The ISC web portal has the additional challenge of integrating policy acceptance from third party organizations. These outside organizations may have conflicting policies or policies that are considered substandard to the needs for the supply chain coordinator.

It is especially important that corporate management fully support the security policy process otherwise there is little chance that they will have the intended impact, no matter where the incident resides. The following list of individuals should be involved in the creation and review of security policy documents:

- Site Security Administrator
- Information Technology Technical Staff

- Administrators of Large User Groups (e.g. Domain organizations, business divisions)
- Security Incident Response Team
- Representatives of the user groups affected by the security policy
- Responsible management
- Legal Counsel

This list is representative, but not necessarily comprehensive. The supply chain coordinator may find as it adds functionality to the web portal that additional representation may be required, especially when integrating third party or member level systems and networks. It may be helpful to bring in representation from stakeholders, management with budget and policy authority, technical staff with knowledge about what can and cannot be supported, and legal counsel that understand the legal ramifications of various policy choices.

Recommended Policies

This section will discuss the specific policy requirements for the web portal. The recommended policies are based on Internet industry standards and best practices for web portal security.

Appropriate Use Policy (AUP)

An Appropriate Use Policy (AUP) may also be part of a security policy. It should spell out what users shall and shall not do on the various components of the system, including the type of traffic allowed on the networks. The AUP should be as explicit as a possible to avoid ambiguity or misunderstanding.

Privacy Policy

Privacy of files and information stored on or within the web portal applications needs to be assured. User information that includes name, address, financial information, and other confidential information may at times need to be shared.

Sometimes during the normal course of operations, a member of the web portal support staff will have a need to view a file belonging to another user of the system. Some examples are: helping a user with an application problem which requires access to the supply chain coordinator's source program; or helping a user resolve an electronic mail problem which requires viewing part of the user's mail message file. Whenever required to view a user's file in the course of helping that user, the consent of the user can be first obtained. In all cases the client should be advised that his/her file(s) may need to be viewed/accessed to assist them.

When assisting web portal users, it is recommended that the Support Staff should use the following guidelines:

- Use and disclose the users data/information only to the extent necessary to perform the work required to assist the user. Particular emphasis should be placed on restricting disclosure of the data/information to those persons who have a definite need for the data in order to perform their work in assisting the user.

- Do not reproduce user's data/information unless specifically permitted by the user.

- Refrain from disclosing a user's data/information to third parties unless written consent is provided by the user.

- Return or deliver to the user, when requested, all data/information or copies to the user or someone they designate.

The privacy policy should define reasonable expectations of privacy regarding other issues such as monitoring of electronic mail, logging of keystrokes, as well as access to users' files.

Access Policy

Clearly defined access policies may be helpful to the success for implementing and sustaining a secured web portal. The ability to grant access rights occurs throughout the levels of security as defined by the business needs for the supply chain coordinator corporate, members, suppliers, and distributors. This complexity forces the need for an effective access policy to assure clear adherence to these business rules.

An access policy needs to define access rights and privileges to protect assets from loss or disclosure by specifying acceptable use guidelines for users, operations staff, and management. It should provide guidelines for external connections, data communications, connecting devices to a network, and adding new software to systems. It should also specify any required notification messages (e.g. connect messages should provide warnings about authorized usage and line monitoring, and not simply say "Welcome").

The web portal has identified several concerns as outlined in the voice of the customer (VOC) section earlier, and from those issues is the following recommended approach for granting, restricting, and monitoring access rights:

1. Ensure a minimum level of consistent access control for supply chain coordinator information assets.

2. Ensure protection of the supply chain coordinator information resources in a manner befitting their value and the risks to which they are exposed. It will assure that:

- Access is granted proactively rather than by default
- Decisions are made by appropriate persons
- Decisions are implemented accurately
- Access control integrity is maintained
- Security violations are monitored and followed up appropriately

1. Ensure that managers of personnel who perform system/security administration functions are responsible for ensuring compliance with this standard.

Note: The Chief Security Officer should recognize that there may be instances where compelling business need warrants use of a system that cannot comply with this standard. It is strongly recommended that requests for exceptions must be approved by the Chief Security Officer.

The following items should be part of the overall access policy, as well as detailed in separate and distinct policy statements (see the following sections):

Authorization

Authorization refers to the process of granting privileges to processes and ultimately to users. This differs from Authentication in that authentication is the process used to identify a user (see next section). Once identified reliably, the privileges, rights, property, and permissible actions of the user are determined by authorization.

In a reasonable security system, it is impossible to explicitly list all of the authorized activities of each user with respect to all resources. The recommended approach is outlined within the section entitled **Technology** (below) that allows for roles and groupings to help manage and maintain the authorization levels for collections of users. The **Technology** section also describes how hierarchies can be implemented to provide greater flexibility for authorization, and expend authorization controls to span of data control as well as application access control.

However a solution is implemented, policies governing authorization should include the following stipulations:

- Requests for access must be properly authorized BEFORE being granted

- A process must be followed to ensure that the authorization is valid. In the case when security administration is done for a large number of users with many authorizers, it may be useful to maintain a list of authorized signers or signatures.

Administration

Administration of access rights should be simple and easy to maintain. Policies that specify administrative users and their access rights and privileges should be clearly defined before assigning responsibilities. Who is responsible for what types of administration activities will be the primary result of definitive access policies specifically for administrators. Certain aspects of access policy will simply the role of the administrator, including the following items:

- The user identifications should be unique within the domain for which a particular administrator is responsible. User identifications are called various names depending on the system used. Examples include: USERID, ID, LOGON ID.

- New passwords should be issued by a process that ensures that they will not be disclosed to anyone other than the intended recipient. If disclosure occurs in the issuing process, the process must detect it.

Activity/Violation Review

It is important to clearly identify within the Access policy that these activities are monitored and tracked. A review process should be in place to assure that the access

rights and privileges are granted appropriately. The following aspects should be addressed in the Access policy:

- Security administration activity must be reviewed to verify its accuracy and appropriateness. This review must be conducted by someone other than the person whose activity is being reviewed.

- Reported security violations should be reviewed daily. Records should be kept to show that the review occurred, by whom it was conducted and what action, if any, was taken.

Record Keeping

If a data processing system is used as a record keeping system, sufficient backup should be provided to allow recovery of the security activity records in case of system problems.

Records that show the person to whom an ID has been issued, the access requested, the person who authorized it, must be maintained.

Records of IDs that have been suspended and reactivated should be maintained. These will assist in detecting users who need more training or IDs that are being used for unauthorized access attempts.

Records of terminated employees' access should be kept on hand for at least six months after termination. After that time period that information may be placed in accessible archives.

Records for security violations should be maintained onsite for a minimum of one month. These records will assist in detecting longer term trend and penetration attempts.

Records should be kept to show system/security administrator activities:

- Have been reviewed
- By whom the review was conducted
- What action was taken to deal with any noted exception conditions

It is important to include policy and procedures for granting access as well as removing access for web portal users.

Remote Access

While Internet-based attacks get most of the media attention, most computer system break-ins occur via dial-up modems. The nature of the supply chain coordinator's membership and access requirements will in most cases use dial-up modem access. Policies and procedures to specify and monitor the method and use of dial-in access need to be stated.

There are a variety of configurations for supporting remote access via dial-up lines and other means. In general, the major security issue is authentication - making sure that only legitimate users can remotely access your system. The use of one-time passwords and hardware tokens is recommended for most companies; however, the supply chain coordinator's web portal user communities may not be able or willing to monitor these remote access devices, particularly due to high expense and difficulty to track.

Another issue is the supply chain coordinator's ability to monitor the use of remote access capabilities. The most effective approach is to centralize the modems into remote access servers or modem pools. This design enables an easier monitoring and tracking of dial-in usage.

For low level security requirements, the following dial-in policy is sufficient:

- All users who access the web portal system through dial-in connections must periodically change their passwords.

However, the supply chain coordinator has set requirements that demand higher levels of security, with information sources beyond just the supply chain coordinator servers, but also at third party locations, so it may become useful to increase the dial-in protection policy statement to the following:

- Direct dial-in connections to the supply chain coordinator web portal systems must be approved by the Operations Support Manager and the Chief Security Officer.

- Information regarding access to company computer and communication systems, such as dial-up modem phone numbers, is considered confidential. This information must not be posted on electronic bulletin boards, listed in telephone directories, placed on business cards, or made available to third parties without the written permission of the Operations Support Manager. The Operations Support Manager will periodically scan direct dial-in lines to monitor compliance with policies and may periodically change the telephone numbers to make it more difficult for unauthorized parties to locate company communications numbers.

Additional policy statements should address encryption within any remote access policy, as suggested in the following:

- All remote access to the web portal system, whether via dial-up or Internet access, must use encryption services to protect the confidentiality of the session. Supply chain coordinator approved remote access products must be used to assure interoperability for remote access server encryption technologies.

Physical Access

It may be useful for the supply chain coordinator to put into place appropriate safeguards to limit physical access to any computer or computer related device. The retailer level access has multiple opportunities for non-authorized access, and may even require physical locks or other types of security devices to prevent theft of equipment. It becomes more important to set policies in place that at a minimum attempt to secure physical access in the following ways:

- Secure Locations. Mainframe, servers and other computer devices may be stored in a location that protects them from unauthorized physical access. Physical access to such equipment potentially provides access to information stored therein. Placing equipment where such access may not be easily restricted does not preclude accountability for such access.

- Location Selection. Physical locations for all computer related equipment should be selected to protect against equipment and information loss by flood, fire, and other disasters, natural or man-made.

- Review of New Connections to Outside Sources. Proposed access to or from a network external to the agency must be reviewed and approved by the organization head or designee prior to establishment of the connection.

- Review of Installation. Installation, upgrade, changes or repairs of computer equipment and computer related devices (hardware, software, firmware) must be reviewed by the organization head for potential physical security risks.

- Platform-specific Physical Security. Platform-specific physical security must be established, implemented and periodically reviewed and revised as necessary to address physical vulnerabilities of that platform.

- Laptop, Notebook and Portable Computer Devices. Portable computing devices must not be left unattended at any time unless the device has been secured. When

traveling, portable computers should remain with the user's carry-on hand luggage.

It is equally important to state within a physical access policy that the accountability for such access is not precluded where exceptions must be made, such as in a restaurant, where locked offices are not common. Users should remain accountable for usage regardless when reasonable attempts have been made to secure physical access to the web portal.

Accountability Policy

An Accountability Policy is needed to define the responsibilities of users, operations staff, and management. It should specify an audit capability, and provide incident handling guidelines (i.e. what to do and whom to contact if a possible intrusion is detected). The previous section outlined procedures for incident handling, and clear accountabilities should be stated in conjunction with those processes.

Authentication Policy

An Authentication Policy establishes trust through an effective password policy, and by setting guidelines for remote location authentication and the use of authentication devices (e.g. one-time passwords and the devices that generate them). Encryption may also be used to authenticate users, as it requires possessing a key to unscramble data, and this policy may apply for some of the more sensitive data exchanges provided through the web portal.

Robust Passwords

In many cases of system penetration, the intruder needs to gain access to an account on the system. One way that goal is typically accomplished is through guessing the password of a legitimate user. This attempt is often accomplished by running an

automated password cracking program, utilizing a very large dictionary, against the system's password file. The only way to guard against passwords being disclosed in this manner is through the careful selection of passwords that cannot be easily guessed (i.e. combinations of numbers, letters, and punctuation characters). Passwords should also be as long as the system supports and users can tolerate.

Change Default Passwords

Many existing security systems and application programs are installed with default accounts and passwords. These should be changed immediately to something that cannot be easily guessed or cracked.

Restrict Access to the Password File

Restrict access to the password file, in particular, the security system should protect the encrypted password portion of the file so that would-be intruders do not have them available for cracking. One effective technique is to use shadow passwords where the password field of the standard file contains a dummy or false password. The file containing the legitimate passwords are protected elsewhere on the system.

Password Aging

When and how to expire passwords may become a subject of controversy among the security community. It is generally accepted that a password should not be maintained once an account is no longer in use, yet it is hotly debated whether a user should be forced to change a good password that is in active use. The opposition claims that frequent password changes lead to users writing down their passwords in visible areas (such as sticky notes on a terminal), or for users to select very simple passwords that provide very little if any protection.

Password Lock-outs / Account Blocking

Some sites find it useful to disable accounts after a predefined number of failed attempts to authenticate. If the supply chain coordinator site uses this mechanism, it is recommended that the mechanism not "advertise" itself. After disabling, even if the correct password is presented, the message displayed should remain that of a failed login attempt. Implementing this mechanism will require legitimate users to contact their system administrator to request that their account be reactivated.

At the supply chain coordinator Member level, it may become cost prohibitive and even an operational nuisance to field the numerous calls that may result from retailer level users locking out of the system. This type of policy may need to be adjusted for effectiveness, as one risks similar issues of writing down passwords in visible locations in order to avoid accidental lock-outs.

Encryption

There will be information assets that the supply chain coordinator will want to protect from disclosure to unauthorized entities. Many existing security systems have built-in file protection mechanisms that allow an administrator to control who on the system may access or "see" the contents of a given file.

A stronger way to provide confidentiality is through encryption. Encryption is accomplished by scrambling data so that it is very difficult and time consuming for anyone other than the authorized recipients or owners to obtain the plain text. Authorized recipients and the owner of the information will possess the corresponding decryption keys that allow them to easily unscramble the text to a readable form. The supply chain coordinator should consider the extent and value of its information assets (as outlined previously) to determine the need for encryption protection.

Additionally, the use of encryption is sometimes controlled by governmental and site regulations, so the supply chain coordinator should encourage administrators to become

informed of laws or policies that regulate its use before employing it. As the specific encryption needs require clearly identified data and information sources, so it is outside the scope of this document to mention various programs available for this purpose. However the recommended solutions in this document include systems that provide appropriate use of encryption.

Availability Statement

An Availability Statement sets users' expectations for the availability of resources. It should address redundancy and recovery issues, as well as specify operating hours and maintenance down-time periods. It should also include contact information for reporting system and network failures.

Information Technology System and Network Maintenance Policy

An Information Technology System and Network Maintenance Policy describes how both internal and external maintenance people are allowed to handle and access technology. One important topic to be addressed here is whether remote maintenance is allowed and how such access is controlled. Another area for consideration here is outsourcing and how it is managed.

Violations Reporting Policy

A Violations Reporting Policy indicates the types of violations that must be reported (e.g. privacy and security, internal and external), and to whom these reports are made. A non-threatening atmosphere and the possibility of anonymous reporting will result in a greater probability that a violation will be reported if it is detected.

Supporting information should provide users, staff, and management with contact information for each type of policy violation; guidelines on how to handle outside queries about a security incident, or information that may be considered confidential or

proprietary; and cross-references to security procedures and related information, such as company policies and governmental laws and regulations.

Functional Requirements

Introduction

The purpose of this section is to specify the capabilities that must be available in the portal to achieve the security related CTQs.

The section will begin by defining some terms that are commonly associated with the management of security and access.

Next the portal will be viewed from the perspective of security and access management to identify the components that are associated with security and access management.

Lastly each component will be described in terms of the specific functions it must provide to effectively secure and manage portal access.

Some features that characterize the capabilities the portal must possess in order to achieve its CTQs will be used to validate each functional component. These features will include the ones that were explicitly cited in the user workshops plus some capabilities that were added after those sessions.

Definitions

This section will set a baseline for functional specification discussion by:

- Defining concepts and terms that are commonly employed to manage security and access.

- Describing each in the context of the portal and it community.

- Specifying, where applicable, how each will be used to manage security and access.

Community

Community refers to all of the users of the portal. The security capabilities will be used manage access within the community.

Domain

A domain is a community subset that relates to a type of user in the portal.

The portal is comprised of the following domains:

- Members (franchisees)
- Distributors
- Suppliers
- Corporate

An individual can belong to one or more domains.

Group

A group relates to an organizational entity in the portal. Examples of groups are a member company or a specific supplier or distributor company.

- Groups belong to domains.

- Groups are made up of one or more data related entities. A retailer is an example of a data related entity.

- Groups can be enabled to create sub-groups. A member regional division that consists of several retailers is an example of a sub-group.

- The reason for having groups is to define authorization. A group specifies the data that can be accessed by the individuals that are associated with the group.

Role

Roles relate to a set of permission within a group.

Examples of roles are:

- Administrator
- Store manager
- Retail outlet owner

Roles can be aligned with a corporate function (e.g. marketing) or other criteria

Reasons for having roles is to define privilege. A role specifies the portal functions an individual can access.

User

A user relates to an individual in the community.

- User will belong to a domain (i.e. member, supplier, distributor or supply chain coordinator).

- User must be associated with one group.

- User may or may not have a role assigned to them.

- A user's access is controlled through the group(s) to which they belong (authorization) and the role that has been assigned to them (privileges).

Hierarchy

A hierarchy is a tree structure that maps to a specific domain entity's organization (e.g. member ABC).

- Hierarchies can apply to groups and/or users.

- Group hierarchies are used to further refine authorization.
    - View data from any point downwards
    - Restrict at intermediate levels below the top group level.

- User hierarchies can be used to delegate permissions or to create users owned by other users (e.g. the relation ship of a district manager to the retailer managers that report to him/her).

Components

Figure **72** shows several applications for the portal **7200**. Users (members, suppliers and distributors) **7202** will access the portal via the Internet. Depending on the portal hosting arrangements, users may access the portal via their internal LAN or through the Internet. Access to the portal and its application will be controlled by the security component **7204**. The security component will be managed by the supply chain coordinator and user administrators who have been designated by the supply chain coordinator.

Figure **73** shows an expanded view of the portal **7300** from a security and access control perspective. The role of each component shown is briefly described.

User Logon **7302**

The user logon component verifies that a user is authorized to access to the portal.

Community Management **7304**

The community management component allows administrators to manage the users in their span of control within the portal. Specifically they can add, change and delete users and they can control what users can view and what functions they can perform.

Policy Management **7306**

The policy management component uses the user authorizations and privileges to verify that a user is authorized to perform a requested function.

Reporting **73O8**

The reporting component provides the administrators with user and activity information that is suitable for managing security and access.

Functions

The purpose of this section is to specify the functions that may be useful for delivering the features for achieving the portal's security related CTQ.

The following factors can be considered in specifying the functions:

- The security features that were identified by the members, supplier and distributors in their workshop sessions. These are the characteristics of the portal that must be present in order to meet their CTQs.

- Additional features that were identified in follow-up review sessions with supply chain coordinator personnel. These are more subtle features that emerged during technical, organizational and authorization discussions.

- Best practices that are frequently employed in system security and access management.

Each functional component will first be described in terms of purpose and general approach. Then details will be provided for each function to specify the capabilities that must be present.

Assuming that the supply chain coordinator desires to use existing 3rd party software as much as possible, the traditional approach of specifying inputs, processing and outputs for each function will not be strictly followed here. Rather, the emphasis will be placed on clearly describing the full set of capabilities that will be required to deliver the features needed to meet the CTQs. The details associated with the specifics of inputs, forms, detailed processing and outputs will vary by vendor and the vendor's approach to providing the necessary capabilities. It will be the job of the vendors to provide these details so that the supply chain coordinator can use them to determine the best approach for their requirements.

Logon (Authentication)

Function Purpose

The logon function represents the first line of security and it validates that a user is authorized to access the portal.

Function Details

The authentication process begins when a user connects to the portal. At that time they will be prompted for:

- Company ID
- User ID
- Password

The user will enter the requested data and it will be encrypted prior to sending it to the portal logon function. Additionally the password field will be masked when the user enters it (i.e. it won't print on the screen when the user enters it).

Once the user has submitted the information, the logon function will check the portal access control list to determine if access is permitted to the companyID/userID/password combination that the user submitted.

Users failing to enter a valid companyID/userID/password combination will be notified of the failure and re-prompted. A userID will be locked out after n failures.

The logon function will provide the following password management capabilities:

- Password disablement after an administrator specified period of inactivity.
- New user must provide a new password the first time they logon to the portal.
- Passwords will expire after an administrator specified period of time and the user will be required to provide a new one.
- Alternate passwords will be provided for lost/forgotten password situations.

New passwords will be subjected to minimum security password validation rules. These will include things like minimum/maximum length, percent of characters that must differ, uniqueness, etc.

Once a user has been successfully authenticated the system will:

- Offer an option to the user to change their password
- Show the date and time the user last sign on to the system (detect stolen user ID and password).
- Retrieve the user's profile data that defines what data and functions the user can access and transfer to the policy management function (i.e. portal main menu).

All details associated with the logon session will be written to the audit log.
The system administrator will be notified of user ID lockout. The following table lists User Specified Features.

Table 9

Feature	**CTQ Category**	**Explanation**
Lockout user after n unsuccessful logon attempts	Security, Prevention	
Notify administrator of lockouts	Security, Prevention	This is a proactive notification that occurs via email, pager, etc. when the attempt occurs
On line monitoring	Security, Prevention	This includes administrator notification of lockout and

Feature	CTQ Category	Explanation
		could be expanded to include other threats or situations.
Provide alternate passwords for lost/forgotten password situations	Flexibility	
Password expiration; require periodic password changes	Security, Prevention	
Acceptable password length parameters	Security	
Ability to assign/select password	Security	User can specify their password and change it any time.
Ability to transfer logon intelligence.	Simplicity	The ability to transfer the user profile information that specifies what data and applications they can access is helpful for supporting a single sign on capability for the portal.
Record all activities to the audit log	Security, Prevention, Reporting	This was not an explicitly stated feature. However, it will be required to support the reporting features that were requested by the users.

Community Management

The community management capability allows administrators to manage the user activities within the portal. Specifically it provides the capabilities to add, change and delete users, and to manage what the user can see and what functions they can perform.

Community management can be covered in four sections:

- *Community/Domain Wide Administration*

  Describes the supply chain coordinator system wide administrative capabilities that will be required to establish the community and the entities that make it up (i.e. members, suppliers, distributors and supply chain coordinator).

- *Basic Delegated Community Management*

  Describes the capabilities that will be needed to achieve the CTQs. Many of the capabilities that are found in this basic model can be accommodated by 3rd party software. Some custom programming will likely be required to manage authorization within the complex organizational structures found at the supply chain coordinator.

- *Group Hierarchical Management*

  Describes the use of hierarchies to manage access. This will achieve many of the simplicity and flexibility related CTQs that were not meet by the basic model. It will likely require custom development.

- *Data Publication*

  Describes a capability that is need to support situations such as joint ownership of stores and corporate board committees. It will enable the owner of a group to permit user in other groups to access data in the owner's group. This will be largely custom development.

Community/Domain Wide Administration

Function Purpose

There are certain capabilities that affect the entire community or all of the occupants of a domain (members, suppliers, distributors and supply chain coordinator). These are limited to a single system wide administrator and potentially to domain administrators.

Function Details

Community and domain wide administration will include the following capabilities:

- *Community wide administration*
  - Add/change or delete a domain.
  - Delegate domain administration to a domain administrator.

- *Domain administration*

  Domains are comprised of organizations (e.g. members). Organizations are made up of data related entities (retailers, distribution center, plants, etc.). The domain administrator needs the following capabilities to create and manage organizations that make up their domain.

  - Add, change and delete data related entities (e.g. retailers).
  - Link data related entities together (e.g. retailers) into an organization (e.g. member).
  - Create an organization administrator and delegate the administration of their organization to them.

Basic Delegated Community Management

Function Purpose

The purpose of community management is to provide a sub administrator with the ability to control what their users can view and what tasks they can perform.

An administrator who has been granted administrative privileges for the sub domain that represents their organization performs community management (e.g. a member's retail outlets make up the member's sub domain).

The basic model provides the administrator with tools that are used to manage a user's access (view and tasks). These tools include:

- Groups to specify span of control.
- Privileges to specify tasks
- Roles to specify a set of privileges that are associated with a function (e.g. retail outlet manager).

Community management then provides the administrator with the ability to add, change and delete users.

Lastly it enables the administrator to control user's view and access rights by associating them with a group of data related entities (e.g. retailer) to specify what the user can see and with a role or specific privileges to specify what tasks the user can perform.

Figure **74** is a flow diagram showing how group and roles manage access. User ABC **7402** is associated with Group 2 and is assign a manager role. This entitles ABC to order F and P and view forecasts for retail outlets 1 and 2.

Function Details

Functional details will be covered in the context of groups, roles and users.

Group Management

As stated earlier, a group is an organizational entity that is made up of one or more data related entities. The retail outlets owned by a franchisee comprise a member group. Groups serve to specify a user's span of control when they are associated with a user.

An administrator who has been authorized to manage groups can create new groups, and change and delete existing groups.

New groups:

- Requires an ID that is unique in the administrator's span of control.
- Requires a descriptive name.
- Entities (e.g. retailers) that are placed in the new group must exist within the administrator's span of control.

In order to change or delete a group, it must exist in the administrator's span of control. Entities being added to an existing group (change) must exist in the administrators span of control.

Role Management

A role is a functional entity that is made up of tasks the function is permitted to perform. A restaurant manager is a role that is permitted (i.e. given a privilege) to perform the tasks of ordering food and packaging, and viewing forecasts.

An administrator who has been authorized to manage roles can create new roles, and change and delete existing ones.

An administrator must possess any privilege they assign to a role.

New roles:

- Requires an ID that is unique in the administrators span of control.

- Requires a descriptive name

In order to change or delete a role, it must exist in the administrator's span of control.

Privileges can be specified as default or optional when they are assigned to a role. Default privileges are automatically given to a user when they are assigned to a role. The administrator must explicitly specify each optional privilege (yes/no) for a user when they are assigned a role.

A role may be assigned to a group as well as to a user. When it is associated with a group, users receive the privileges specified by the role when they are associated with the group.

User Management

A user is an individual who is authorized to perform some set of tasks on behalf of a group (e.g. a set of retail outlets).

An administrator who has been authorized to manage users can create new users, and change and delete existing ones.

A company ID, a user ID and a password identify a user. The administrator cannot view the user password.

New users:

- Require a user ID that is unique in the sub domain (e.g. unique within a member organization).
- Require an email address.
- Require a descriptive information such as name and address name.
- The system will assign the password to a new user and inform them of it via email.

User span of control:

- The administrator specifies a user's span of control by associating the user with a group(s) that represent the desired span of control.
- The administrator can associate (add) and disassociate (remove) users with groups.
- In order modify a user's span of control, the user must exist within the administrator's span of control.
- In order associate a user with a group, the group must exist within the administrator's span of control.

User/group application access:

- The administrator specifies the application a user/group can perform by assigning roles/privileges to the user/group.
- The administrator can add and remove roles/privileges from users/ groups.
- In order assign a role to a user/group, the role must exist within the administrator's span of control.
- In order modify a user roles/privileges, the user must exist within the administrator's span of control.
- An administrator must possess any privilege they assign to a user/group.
- If a role is being assigned to a user/group, and if the role has optional privileges, the administrator will be shown the optional privileges and allowed to remove ones that they don't want to grant to the user.

Other

All details associated with community management activities will be written to the audit log.

A capability to link community management with the supply chain coordinator's member management system is required to eliminate duplicate data entry and keep the two systems synchronized.

5 A batch bulk load capability is required to enable user to export data from existing systems to set up their organization in the portal community.

Table 10

Feature	**CTQ Category**	**Explanation**
Distributed community administration	Flexibility	Users need to be able to manage their users and their access within the portal. They don't want to be dependent on the supply chain coordinator.
Ability to add, change and delete users.	Security, Flexibility	
Ability to assign access to users	Security, Flexibility	Specify span of control and privileges
Ability to create roles or level of users	Simplicity, Flexibility	
Ability to set up default levels of access	Simplicity, Flexibility	
Ability to clone and/or access rights	Simplicity, Flexibility	
Mass delete of users	Simplicity, Flexibility	Not provided as a part of community management.

Ability to copy a user ID	Simplicity, Flexibility	Provide to extent that a user's access attributes can be easily specified through groups and roles
Ability to export user load information from member backend.	Cost	Large member would like to use existing data to establish/maintain their organization in the portal.
User can be associated with multiple groups.	Flexibility	District manager A is a backup for district manager B. As a result, A will need to perform ordering district A and B and will need to be associated with both groups. Feature will also be required to support organizations such as finance who will need to view the data of several groups.

Hierarchy

Function Purpose

The basic community model that was outlined in the previous section supported authorization and access management for a flat single level organization. Although this can be adapted to support a multi-level organization, it falls short on the CTQs related to simplicity and flexibility. Specifically, the administrator must create groups to correspond to each span of control. This results in a single entity having to be included in several groups. For example, a single retailer may be included in a district, region and a corporate group. Administration in a scenario like this is complex and labor intensive. It becomes particularly cumbersome and error prone because things like an organization change (e.g.

new retail outlet) requires the modification of several groups (i.e. add it to district, region and corporate group).

A hierarchy provides a superior way to manage span of control and access. The hierarchy defines a company's organization. A user's span of control is set by associating them to the node of the hierarchy that corresponds to their position in the company. This association authorizes them to view the data associated with any entity that belong to the node to which they are assigned. In the case of a new retail outlet, assigning it to a manager also places it in the span of control of the manager's district and region mangers and the corporate CEO.

Hierarchies can also simplify the specification of user privileges by associating them to a hierarchy.

Although hierarchies introduce technical complexity, they greatly simplify administration in large and complex organizations.

The following outlines the requirement details associated with hierarchies.

Function Details

A hierarchy is made up of nodes where a node represents a business function (e.g. retail outlet manager, district manager, etc.). The bottom nodes of a hierarchy are associated with a data related entity (e.g. retail outlet is associated with a manager node/function). They are then grouped under nodes at successively higher levels (e.g. districts, regions, etc.). The top of the hierarchy is a single node (e.g. corporate). In a hierarchy an entity (e.g. retail outlet) will appear in the span of control of each successive parent node.

The following administrative capabilities are required to manage authorization and access with hierarchies.

Hierarchy Management

- Add a node

  Specify a parent node in a hierarchy and add a node beneath it.

- Delete a node

  Specify a node in a hierarchy and delete it. This also results in the deletion of any dependent nodes reporting to the node that was deleted.

- Move a node

  Specify a node in a hierarchy and move it and its dependents to another node (drag and drop).

- Associate a data entity with a node

  Specify a node in a hierarchy and associate a data related entity to it (e.g. retailer) with it. In this situation, no nodes can exist beneath the node specified. Also the data related entity must exist in the administrator's span of control.

- Disassociate a data entity with a node

  Specify a data related entity in a hierarchy structure and delete it from it parent node.

- Move a data entity from one node to another

  Specify a data related entity in a hierarchy structure and move it from its present parent node to a new parent node (drag and drop).

User Span of Control Management

Span of control relates to the data a user can view. Under a hierarchy, associating a user to a node in a hierarchy specifies their span of control. This association entitles the user to view the data associated with any entity that is found in the user's node group.

User Access Management

Access management relates to the functions a user can perform. It is controlled by privileges and roles that are assigned to a user (groups of privileges). Under a hierarchy, roles and privileges can be associated to a node. Any user who is then associated to the node receives the privileges that accompany it. See the table below.

Table 11

Feature	**CTQ Category**	**Explanation**
Ability to publish rights and privileges across hierarchies.	Simplicity, Flexibility	
Ability to authorize multiple levels of a hierarchy	Simplicity, Flexibility	
Ability to manage access against hierarchies	Simplicity, Flexibility	
Flexible data access and management.	Simplicity, Flexibility	

Data Publication

Function Purpose

Portal data (e.g. a retailer) is owned by one and only one sub domain entity (e.g. member). The ability to view and process that data is restricted to users and groups who inhabit the entity's sub domain and who have been authorized to do so by its administrator.

However, there are several business situations where an organization needs to view and process data that is owned by another organization that may or may not belong to the same domain. Some common examples are:

- Two members share ownership of a retailer. As a result both members need to view information about the jointly held retail outlets and order supplies for them.

- Members belong to the supply chain coordinator board or corporate committees. In order to participate in these roles the members need to view and potentially access data in the supply chain coordinator's domain.

The data publication capability is a mechanism for the owners (e.g. member A) of an entity (e.g. retailer 123) to permit a users in another organization (e.g. member B) to view and access the entity's (i.e. retailer 123) data.

Function Details

Data publication is an administrative privilege. It is used by a data owner's administrator to setup a relationship with another party in the portal that will allow that party to view and access data entities (e.g. retailers) that are found the owner's sub domain.

The data publication function will possess the following capabilities.

- The administrator can add, change or delete a data publication relationship.

- Any data entity that is published must exist in the administrator span of control.

- The following elements will be provided to specify a data publication relationship.

    - The span of control (view) that is associated with a data publication. The span of control may be specified as an individual entity (e.g. a retailer), a group (e.g. a district) or a hierarchical node (if a hierarchy feature is provided).

- Privileges or functions the receiver can perform with the published data.

- The domain (i.e. member, supplier, distributor, supply chain coordinator) and sub-domain ID (company ID) of the organization to which the data is being published.

- The group or node ID in the receiving organization that the published data will be associated with.

- The user ID of the person in the receiving organization who will own the data. This person will control the user views and access (privileges) associated with the published data in their organization.

- All details associated with creating or modifying a data publication relationship will be written to the audit log.

The following table sets forth User Specified Features:

Table 12

Feature	**CTQ Category**	**Explanation**
User can view or access data in another sub-domain in their domain.	Simplicity Flexibility	Joint ownership of retail outlets by distinct members.
User can view or access data in different domain.	Simplicity Flexibility	Support board of directors and committees that require members to view and access supply chain coordinator corporate data.

Policy Enforcement

Function Purpose

The policy enforcement function is a centralized capability that manages access to all of the applications that comprise the portal.

Policies specify the access requirements for each application that makes up the portal. The policy enforcement function determines if a requesting user meets the access requirements for an application. The user is granted access by the policy enforcement function if they meet they requirements specified by the policy.

Function Details

A central administrative capability is required to maintain the policies that are used to manage access to the portal's applications.

The details associated with policy enforcement are as follows:

- When a user successfully logs on to the system by providing a valid user ID and password, their span of control and application privileges are retrieved.
- The user is presented with main menu for the portal.
- The user requests a function from the menu.
- The policy enforcement function retrieves the access policies for the requested application from the central policy repository.
- The user's span of control and application privileges are evaluated against the application's policies.

- If the user satisfies the requirements specified by the policy, access is granted.

- If the user does not satisfy the requirements specified by the policy, access is denied.

- Details associated with an access request are recorded in the central audit log.

- The policy enforcement function is responsible for interfacing with the portal applications and passing them information about the user that they require.

The following table sets forth User Specified Features.

Table 13

Feature	**CTQ Category**	**Explanation**
Single sign on	Simplicity	After signing on to the portal, the user can access all applications that make up the portal.
Ability to integrate with affiliates (i.e. other 3rd applications that make up the portal).	Simplicity Integration Cost	Provide the affiliate application with the user information it requires to function. Prevent redundant data entry, redundant security, etc.
Ability to interface with other applications: supply chain coordinator 3rd party Remote hosts	Simplicity Integration Cost	The supply chain coordinator wants to use 3rd parties and application service providers (ASPs) for their portal applications. The policy

Feature	CTQ Category	Explanation
Platform independent		enforcement manager must be capable of interfacing with a variety of platforms in a variety of situations.
Centralized policy management	Simplicity Integration Cost	Don't want redundant application access permission management.

Reporting

Function Purpose

The portal must provide its administrators with two forms of reporting:

- Community management reports.
- An event reporting capabilities that provides the administrator with the data and tools for researching issues, problems, potential breaches, etc.

Functional Details

The functional details of reporting will be covered from the perspective of report type.

Community Management Reports

Community management reports provide administrators with the information they need to manage their users, groups, roles and hierarchies (if implemented).

Reports will likely include:

- User information report showing things such as:

- Basic user information (name, address, telephone number, etc.)
- User span of control
- Roles/privileges
- Usage data (date of last logon, number of logons, total logon time, average logon time, etc.)
- User lockout

- Group reports showing thing such as:

  - The entities (e.g. retailers) that make up a group.
  - Role associated with a group.
  - Users associated with a group.

- Role reports showing things such as:

  - Default and optional privileges associated with each role.
  - Groups associated with each role.
  - Users assigned to each role.
  - Users assigned to each available privilege.

Report content will be limited by the administrator's span of control.

Query and filter capabilities will be required to specify report type and content (e.g. a specific group, a range of users, all roles, user usage details for date range, etc.).

Event Reporting

An event is a system activity that is written to the audit log. Examples of events include connection to the portal, logon attempt, application access requests, add a new user, system errors, etc. Information will accompany an events that identifies it, identifies the user that initiated it, the date and time the event was initiated, status (success/failure), etc.

Events are recorded so that the details associated with them are available to research problems, security breach attempts, etc.

An alert capability is required to specify administrator notification (email, page, etc.) in the case of certain events (e.g. attempted breach, a portal application is unavailable, etc.).

Because event reports from the audit log are run in response to problems or issues, good filtering capabilities will be required to eliminate unneeded data and provide the administrator with only the information they are seeking. Filters should include user(s), event, and date and time.

The following table sets forth User Specified Features.

Table 14

Feature	**CTQ Category**	**Explanation**
The following community management reports were identified: Master user list Click and view access list User with published data authorization (i.e. users in other domains or sub-domains. Usage reports	Security Reporting Prevention	
Lockout notification	Security	
Online monitoring capability	Security Reporting Prevention	
View audit log	Security	

Feature	CTQ Category	Explanation
	Reporting Prevention	
Parameter driven reports	Simplicity	

Technology

Component and Actor definition of the supply chain coordinator web portal

As detailed in the previous section, the supply chain coordinator's portal may allow access to supply chain applications. The nature of the applications require a feature and function set; this engagement collected CTQs and functions from the community and organized them along categories.

This section places a slightly different view of requirements on the portal. There may be a public site and a private site (secured access); there may also be applications behind the portal provided by 3rd party application service providers that fall under the private site. There may be administration pages to setup authentication and authorization policies. It is also a requirement that the portal support communications between the supply chain coordinator and the community and between community members.

System View Components

Some functional components that may comprise the Portal:

- PVC: Public View Component
- SVC: Secure View Component
- AC: Administrative Component
- CUC: Contact Us Component

A more detailed description of each of these components is stated in the following sections.

Public View Component

The Public View Component describes the functionality that is available to users of the public web pages on the supply chain coordinator portal.

Secure View Component

The Secure View Component describes the functionality that is available to users once they have logged onto the private pages of the supply chain coordinator portal. The private pages include access to the Applications and other functionality.

Administrative Component

The Administrative Component describes the functionality that allows users to access administrative links available to Company Administrators and individual Users. Additionally, the component contains information required for users to log on and request passwords.

Contact Us Component

The Contact Us Component describes the functionality and information that is available to users on both the public and private pages of the supply chain coordinator. This information consists of service-related questions and other areas of concern for community members.

Actor Definition

An actor is a user that plays a role with respect to the system. It is someone or something outside the application that interacts with the supply chain coordinator portal. The defined use cases and their definitions are specified below.

The systems 'Actors' are the different types of people involved in the business process. Earlier, several types of users are defined for each customer type (supply chain coordinator member, supply chain coordinator, supplier, distributor, retail outlet manager). While those are separate organizations, the actors in each share qualities at this high level of definition. The actors for the supply chain coordinator exchange portal are:

- Company Administrator (Tier 1 Registered User; Access to public and private pages)
- Exchange User (Tier 2 Registered User; Access to public and private pages)
- Non-Registered User (Tier 3; Access to public pages only)
- Content Manager (CM, Internal GXS/RM User who has permissions to submit updated content; Access to public and private pages)
- Internal Administrator (Internal GXS/RM User who has permissions to run reports validate the registration status of potential customers; Access to public and private pages)

Actor Details

Company Administrator; (Tier 1 Registered User; Access to public and private pages)

Description: A *Registered User (Tier 1)* is a registered community member who has Company Administrator responsibilities for their account.

Computer skills: Computer skill can vary, but a general knowledge of the Web is assumed.

Business Knowledge: Knowledge of products and services related to the supply chain coordinator suite of applications. This User may be responsible for setting up roles/responsibilities/permissions for Tier 2 Users in the account and company.

Exchange Level User; (Tier 2 Registered User; Access to public and private pages)

Description: A *Registered User (Tier 2)* is a registered user who has the second level of privileges. Tier 2 Users may use applications for which they are registered, but they may not sign up for additional applications without approval from their Tier 1 User.

Computer Skills: Computer skill can vary, but a general knowledge of the Web is assumed.

Business Knowledge: Knowledge of products and services related to a solutions suite of applications.

Non-Registered User; (Tier 3; Access to public pages only)

Description: A Non-*Registered User (Tier 3)* has access to the public pages of the supply chain coordinator. They may be able to register via their company administrator, (if the company has registered) or they may be able to register via the automated registration process (an option described in the upcoming sections). Until they are registered, Tier 3 users may not have any level of access to the private pages of the supply chain coordinator.

Computer Skills: Computer skill can vary, but a general knowledge of the Web is assumed.

Business Knowledge: Knowledge of products and services related to the solutions suite of applications.

Content Manager

Description: A *CM* is a Content Manager who has been authorized to add/update content to the portal, pertaining to the particular products they own.

Computer skills: Computer skill can vary, but a general knowledge of the Web is assumed.

Business Knowledge: Knowledge of products and services related to the solutions suite of applications.

Internal Administrator

Description: An Internal Administrator is a registered user who has been authorized to access certain report generation functionality on the private pages of the supply chain coordinator. They may be the only users allowed to view certain links related to report generation (Similar to Content Managers and the Upload Content Link).

Computer skills: Computer skill can vary, but a general knowledge of the Web is assumed.

Business Knowledge: Should be at the RailMarketplace.com, Inc. or GXS executive or marketing level, interested in site usage and feedback for further enhancements.

Portal Components and Requirement Index

The following section is an attempt to outline the requirements expressed by stakeholders/subject matter experts (SMEs) associated with the supply chain coordinator portal. These requirements revolve around the feature/function lists collected in meetings with the supply chain community as addressed in the previous sections. This list should be considered proposed at this point and based on GE's interpretation of the features collected. IT may be finalized through prioritization and solution decisions. It may be

further refined by the design process that the organization chosen to deliver this solution must complete during implementation.

A listing of these component areas along with their index key is provided below. Table 15 provides a listing of functional requirements so that they can be easily found.

Index Key

PVC: Public View Component
SVC: Secure View Component
AC: Administrative Component
CUC: Contact Us Component

Table 15

Req. ID	Requirement Name	Included in Approach
Public View Component		
UC-PVC.01	View Public Site	
UC-PVC.02	View supply chain coordinator press releases	
UC-PVC.03	View Service Info	
UC-PVC.04	View Media Coverage/Latest News	
UC-PVC.05	Request to Register	
UC-PVC.06	View Legal Pages (Extends from PVC.06)	
UC-PVC.07	View About Us	
UC-PVC.08	View Site Map	
UC-PVC.09	View FAQ's	
UC-PVC.10	Submit Feedback	
Secure View Component		
UC-SVC.01	View Secure Welcome Page	

UC-SVC.02	Select Application	
UC-SVC.03	Launch Application	
UC-SVC.04	View Application Request Form	
UC-SVC.05	Submit Application Request Form	
UC-SVC.07	View "Community Directory"	
UC-SVC.08	Search "Community Directory"	
UC-SVC.09	Community Directory- New User Listing	
UC-SVC.10	Submit Feedback	
UC-SVC.11	Submit User Survey	
UC-SVC.12	Register for Training	
UC-SVC.13	Quit Private Pages	
UC-SVC.14	View Press Releases	
UC-SVC.15	View Service Info	
UC-SVC.16	View Media Coverage/Latest News	
UC-SVC.17	View Site Map	
UC-SVC.18	View FAQ's	
Administrative Component		
UC-AC.01	Login	
UC-AC.02	Submit "Password" Reminder Request	
UC-AC.03	Re-set Password	
UC-AC.04	Submit "Administration" Change Request	
UC-AC.05	Add Content	
UC-AC.06	Submit "User Information" Change Request	
UC-AC.07	Generate User Report	
UC-AC.08	Generate Site Activity Report	
UC-AC.09	Clone User	
UC-AC.10	Mass Delete of Users	
UC-AC.11	Create and Manage Hierarchies	
UC-AC.12	Manages Access Rights Relative to Hierarchies	
UC-AC.13	Grant Privilege to Another User	

UC-AC.14	View Master User List	
UC-AC.15	View Access List	
UC-AC.16	View Users Who Can Access My Company's Data	
Contact Support Component		
UC-CUC.01	Submit Tech Support Feedback	
UC-CUC.02	View Tech Support Main Page	
UC-CUC.02	Access Email ASP	
UC-CUC.04	Submit Press Analyst Questions	
UC-CUC.05	View Business Development	
UC-CUC.06	Submit Billing Questions	
UC-CUC.07	Submit Accounts Payable Questions	
UC-CUC.08	Verify Account Information	
UC-CUC.09	Submit "Other" Questions	

Technology Options

Now that the features have been defined and categorized, and the portal components and actors are known, technology must be selected to address high priority items such as integrating affiliate sites, central policy management, and distributed user administration. Considerations for this selection may include the following IT strategy drivers:

Integrating existing and new security systems

- Integrating existing applications with new Web-based applications
- Providing a seamless integration between portal and affiliate sites
- Delegated and single-point administration
- Centralized security management
- Scalability of the integrated security systems

This list of general drivers matches up well to the feature list as collected:

- Distributed User Administration
- Administrative Audit Trail
- Access Management
- Logon/Password Management
- Reporting
- Policy Enforcement
- Data Management

Security is a major concern, as web sites may contain proprietary business information such as news, data/information, and procurement systems. Without adequate security, opportunities are presented for inappropriate dissemination of proprietary information, sabotage, and other mischievous acts.

Comprehensive Security for the supply chain community breaks down into three areas: Web, Network, and Security. Each of the features extends across all three areas, as the following chart illustrates.

Figure **75** is a schematic illustrating features **7502** and functions **7504** across web **7506**, network **7508** and system areas **7510.** Each area is very important to a strong security policy that may allow the supply chain coordinator to operate in a real-time integrated supply chain mode, but community management at the web layer was the main focus of this engagement and where most of the options and decisions need to be made.

Technically, from the web portal view, there are two main approaches to meeting the CTQs of the supply chain communities. The first option is for the supply chain coordinator to use its existing NT infrastructure. The second option involves purchasing a portal management solution to abstract user management from applications.

- Using the existing NT infrastructure

- Using the basic functionality of the portal management solution with minimal configuration

If option 2 is selected, there are two additional levels of implementation that are additive to option 2. These may be overall options 3 and 4:

3. Further development within the portal management solution to add additional features

4. In addition to extension of the portal management solution, creating custom developed community administration features in a relational database that are matched to the portal directory structure

There is a choice to be made between approach 1 and 2. Approaches 2 through 4 build on each other, with approach 4 including all the functionality of choices 2 and 3 as well. Within choice 2, 3, and 4, there are also sub-decisions to make about products or level of customization. Table 16 illustrates chart comparing options and product/customization levels.

Table 16

Option 1	**Option 2**	**Option 3**	**Option 4**
Use current NT security solution	Netegrity or Securant Security Management Solution Software	Security Management Solution Software + Custom Administration	Security Management Solution Software + Custom Administration + Advanced Community

			Structure

The technology portion of this report may provide a section on each approach. The technical architecture for each may be detailed, as well as decisions that can be made by the supply chain coordinator within each. Each section may then compare the functionality pieces outlined in the section entitled **Fundamental Requirements** to that provided by the approach being described. Finally, costs and level of effort for each approach may be included at the end of each section.

After each web portal approach is documented, sections on network and application development recommendations may also be included.

Option 1: Using Internal NT Security

Solution Overview

The supply chain coordinator already manages Windows NT user accounts for all the employees of the supply chain coordinator. This is to control access to internal business applications. The IT team has the ability to create and delete users, assign user groups, and assign privileges to either the individual user or the user group. Access Control Lists manage the resources each user or user group can access, as well as the level of access such as Read, Write, or Execute. These are some of the same functional requirements for the integrated supply chain portal.

Moving to Internet based systems in the NT environment, most applications developed using Microsoft languages and methods run with Microsoft IIS as the webserver. IIS has authentication functionality included. IIS also provides a authorization features as well such as Read and Write, and since IIS runs as a service on top of Windows NT, it relies heavily on Windows NT user accounts and the Windows NT File System.

This is the approach the supply chain coordinator uses for the pilot web portal system. The supply chain coordinator has created an NT domain for the web application to use. The supply chain coordinator is setting up user accounts in this domain, and the web application is validating users against Windows NT.

Figure **76** is a schematic diagram **7600** showing a current validation of users on a web portal.

For data access in the current web portal, there is an association of retailers to specific supplier, distributors, or supply chain members. This resides in a supply chain SQL database **7602**. The application itself logs onto the database and queries the requested information, using the user id **7604** as a key to make sure the proper data is retrieved for presentation back to the user.

There are ways that the supply chain coordinator could continue this operation to manage the entire community of supply chain users. This would involve centrally administering users and physically adding them to the NT user base. The supply chain coordinator would own validating users and setting up access rights, and would need to communicate frequently with companies (supply chain members, suppliers, distributors) to make sure that user setup was proper.

In order to integrate 3rd party provided applications, custom integration would be required in the link between the supply chain portal and the ASP application. The supply chain could work a transfer of user information in the http headers of linked websites. This would provide for an authentication of the user on the 3rd party site. After the initial transfer, the user would interact with the 3rd party application directly with zero visibility back to the portal. Each 3rd party application would also need to manage users themselves and make sure that their user directories were synchronized with the supply chain coordinator. A way around this is for the third party application to trust that the user being passed is valid and to pass all application-specific data to the application at the

time of the link. This provides an easier administration in this model but a much lower level of security and is not recommended.

Reporting would be handled by the IIS logs. If community members wanted to know what their employees were doing on the supply chain applications, they would need to submit a request to the supply chain coordinator. The supply chain coordinator would then need to manually check their logs and find out what user activities occurred. If a community member wanted to know what activities were performed on a 3rd party hosted application, the supply chain coordinator would then need to contact the 3rd party provider and have them manually search their logs and provide reports back to the supply chain coordinator which could then be shared with the community member.

Comparison to Requested Functions

In a previous section, the features requested by the supply chain community were detailed along with the functions those features imply. The following table shows whether functions are provided by this approach along with an explanation. Table 17 illustrates features within option one.

Table 17

Feature	**Y/N**	**Explanation**
SECURITY		
Lockout user after n unsuccessful logon attempts	Y	Application can be written to lockout after n successful tries
Notify administrator of lockouts	Y	IIS log should capture failed attempt. Application can capture lockout event and write to NT log
On line monitoring		Lockouts are captured in the NT log.
Provide alternate passwords for		

Feature	Y/N	Explanation
lost/forgotten password situations		
Password expiration; require periodic password changes	Y	This can be configured in NT and added to application with minimal development
Acceptable password length parameters	Y	Included in NT
Ability to assign/select password	Y	The supply chain coordinator would create in IIS
Ability to transfer logon intelligence.	N	Not part of NT; a custom integration effort is required per additional 3rd party application.
Record all activities to the audit log	N	Only activities for applications the supply chain coordinator hosts can be captured.
COMMUNITY MANAGEMENT		
Distributed community administration	N	The supply chain coordinator must manage the community centrally
Ability to add, change and delete users.	Y	The supply chain coordinator would perform centrally
Ability to assign access to users	Y	Access Control Lists could be setup in NT
Ability to create roles or level of users	Y	NT allows user groups. Levels beyond that are not supported.
Ability to set up default levels of access	Y	Read or Write
Ability to clone and/or access rights	Y	NT can be configured to allow this.

Feature	Y/N	Explanation
Mass delete of users		
Ability to copy a user ID	Y	There are workaround to enable this using NT.
Ability to export user load information from member backend.	N	Details would be needed and sent to the supply chain coordinator for a custom load
User can be associated with multiple groups.	N	Here groups refers to corporate organizations, and NT structure makes all users part of the same organization within an NT domain.
Hierarchies	N	NT security does not support complex hierarchical structures.
Ability to publish rights and privileges across hierarchies.	N	No hierarchies.
Ability to authorize multiple levels of a hierarchy	N	No hierarchies
Ability to manage access against hierarchies	N	No hierarchies
Flexible data access and management.	N	NT provides very rigid security structures
DATA PUBLICATION		
User can view or access data in another sub-group in their domain.	N	Data is within a domain.
User can view or access data in different domain.	N	NT has single domain.
POLICY ENFORCEMENT		
Single sign on	N	A workaround for SSO is detailed in the section above, but IIS and NT are

Feature	Y/N	Explanation
		not SSO products.
Ability to integrate with affiliates (i.e. other 3rd applications that make up the portal).	N	Not supported.
Ability to interface with other applications: the supply chain coordinator 3rd party Remote hosts Platform independent	N	Not supported
Centralized policy management	N	This refers to all policies for multiple applications. NT security manages policies for all applications running on in the NT domain, but not applications outside of it.
REPORTING		
The following community management reports were identified: Master user list Click and view access list User with published data authorization (i.e. users in other domains or sub-domains. Usage reports		The NT admin can view some of these reports, but they would not be available to the general community as this requirement specifies.
Lockout notification	Y	NT admin can see lockout notification.
Online monitoring capability	N	Not available through web. Available to NT admin on admin desktop.
View audit log	Y	Admin can view

Feature	Y/N	Explanation
Parameter driven reports	N	Not provided to community users.

It is possible to custom develop additional authentication and access control functionality on top of NT-based applications. Code can be written in ASP to provide this additional functionality, which would provide a portion of the functionality included in the products considered for option 2. For the purpose of this study, however, it is assumed that the cost of such development would greater than the cost of option 2, purchasing a portal management solution.

Costs and Timelines for Option 1

In terms of up front cost, this is the supply chain coordinator's lowest cost alternative. The NT administration features already exist, the supply chain coordinator has skilled NT administrators, and the equipment is already in place. An additional server may be required to handle the number of portal requests once the applications are fully available and ramped.

However, this approach fails on several fronts including application integration and distributed administration. Therefore, the supply chain coordinator would need to manage the community centrally with this alternative. The supply chain coordinator would need many administrators to manage the community with this approach, so that should factor into the ongoing costs of this approach.

Option 2: Implementing a Portal Management Solution

Two shortfalls of using the internal NT approach are:

- The supply chain coordinator would only be able to have one set of business rules apply to each user

- Users would need to be managed centrally.

These shortfalls are especially critical considering the supply chain coordinator is planning to outsource many of the applications behind the portal to ASP providers. In a sense, the supply chain coordinator may become an ASP integrator. With this in mind, a component of a solution is providing a clear method for the supply chain coordinator to deliver ASP model services to members and trading partners with distributed administration.

Extracting User Management From Applications

Option 2 is based on a layer of abstraction between security and the supply chain coordinator's applications. Doing this entails purchasing a security management solution that offers single sign-on and the ability to create a unified directory for users across applications. The benefit of the unified directory is the ability to enable the same user to belong to multiple applications (managed by different community owners) without the need to manage the user as many separate users. For example, the supply chain member could belong to the supply chain board community to access board-related reports. The same user may be a user of a supply chain service application, such as order management. In addition, the supply chain member may be enabled to access collaborative applications such as email. The issue, however, is that each application has its own set of privileges and roles that drive business process.

In a single-entity model, such as option 1, roles are defined and users are assigned privileges and roles. However, the defined privileges and roles are pervasive across all applications that are accessed by that sign-on. Allowing the same user to have a single sign-on with different roles based upon the application community they are interacting with (even the same physical application in two different communities) is not possible. This is possible if the supply chain coordinator chooses to implement a single sign-on infrastructure including a unified directory environment, as the community is separate

from the directory that defines the users. Figure **77** graphically shows how user roles are managed in a multi-community environment **7700**.

The separation of community **7702** and directory **7704** also allows the administration in each community to be different even though the user is shared. Consider the example presented earlier in this section. The supply chain coordinator's IT may control administration for board member reports, while the actual community member controls administration for the order management application. The separation allows changes to a user's profile in one community without impacting the user's existence in another. This is especially useful when adding and removing users. The supply chain coordinator may want to remove a user from the ASP order management service but still have them exist in the board member report application

Single Sign-on Definitions

To discuss single sign-on, central policy management, and delegated administration, it is important to define two terms.

Authentication – First step in single sign-on. Uniquely identify a user based on company id, user id, and password.

Authorization – Occurs after authentication. The level of application of data access allowed for an individual user.

Portal Management Solutions

As the integrated supply chain concept caught on, organizations had to deal with the challenges of single sign-on and distributed administration. These are the same issues the supply chain coordinator is dealing with as they begin their initiatives. The first response of large community owners was to custom build solutions on top of their IIS or Netscape server-based applications, as was suggested as possible in option 1. But as organizations

began to build custom solutions, there were many failures or limitations on what could be accomplished. At the same time, the market has matured as the need for SSO and distributed organizations expanded to more organizations. Off-the-shelf single sign-on portal management solutions came to market, and many owners of large communities have replaced their homegrown systems with solutions based on these products, which have the following features:

- User entitlement management
- Authentication with single sign-on
- Distributed and delegated user administration (group level responsibility)
- Affiliate Services (integrate ASPs)
- Centralized privilege management (one place for all applications)
- User tracking (configurable)
- Ability to link attributes for personalization to single sign-on
- Distributed and delegated portal administration
- Integration with most directory services

Web-based Single Sign-on/Portal Management Architecture

SSO/Portal Management products are software packages that run on their own server. They also require a directory to operate against. This can be either LDAP or database directories.

The interaction between applications and the SSO/Portal Management server is client-server based, with the application webserver using an agent or plug-in (client) to reference the central policy server for user validation.

Figure 78 illustrates a schematic **7800** showing the protection of resources with a central policy server, a separate user directory, and the integration of affiliate sites **7802** through the agent client **7804**.

Technologies Supported by SSO Products

Within each area of the architecture, there are multiple methods supported. Solutions can run on multiple operating platforms and with multiple types of user directories. Solutions can be extended with multiple development languages, support many authentication technologies, and operate in conjunction with many network security implementations.

Policy Based Security

Figure **79** illustrates a policy based security architecture **7900**, in accordance with one embodiment of the present invention. One of the features of SSO/Portal Management solutions is central policy enforcement for distributed resources. Historically, policies and users were all managed in the same data store as the application being used. In the SSO model, a layer of abstraction exists where administrators manage policies in one repository and users in another. Applications then access the policy server **7902** (which references the policy and user repository) through an agent. The policy server returns an allowed and denied status.

When purchasing an off-the-shelf product, the infrastructure above is part of the solution. The work that must be performed is setup user and policy management, and then to actually create the users and the policies.

Comparison to Requested Functions

In a previous section, the features requested by the supply chain coordinator's community were detailed along with the functions those features imply. The following table shows whether functions are provided by this approach along with an explanation. Table 18 illustrates the various features associated with option two.

Table 18

Feature	Y/N	Explanation
SECURITY		
Lockout user after n unsuccessful logon attempts	Y	Supported
Notify administrator of lockouts	Y	Supported
On line monitoring		
Provide alternate passwords for lost/forgotten password situations		
Password expiration; require periodic password changes	Y	Supported
Acceptable password length parameters	Y	Supported
Ability to assign/select password	Y	Supported (not self-registration)
Ability to transfer logon intelligence.	Y	Agent to integrate affiliate sites.
Record all activities to the audit log	Y	Supported
COMMUNITY MANAGEMENT		
Distributed community administration	Y	Basic in this option.
Ability to add, change and delete users.	Y	Supported
Ability to assign access to users	Y	Supported
Ability to create roles or level of users	Y	Supported
Ability to set up default levels of access	Y	Supported
Ability to clone and/or access	Y	Supported with configuration

Feature	Y/N	Explanation
rights		
Mass delete of users		
Ability to copy a user ID		
Ability to export user load information from member backend.	N	Supported, but not implemented
User can be associated with multiple groups.	N	Groups here refers to organizations, which required customization
HIERARCHIES		
Ability to publish rights and privileges across hierarchies.	N	No hierarchies
Ability to authorize multiple levels of a hierarchy	N	No hierarchies
Ability to manage access against hierarchies	N	No hierarchies
Flexible data access and management.	N	SSO out of the box does not deal with application-specific access (data required with an application)
Data Publication	N	Not supported
User can view or access data in another sub-domain in their domain.	N	Not supported
User can view or access data in different domain.	N	Not supported
POLICY ENFORCEMENT		
Single sign on	Y	Supported
Ability to integrate with affiliates (i.e. other 3rd applications that make up the portal).	Y	Supported

Feature	Y/N	Explanation
Ability to interface with other applications: The supply chain coordinator 3rd party Remote hosts Platform independent	Y	Supported
Centralized policy management	Y	Supported
REPORTING		
The following community management reports were identified: Master user list Click and view access list User with published data authorization (i.e. users in other domains or sub-domains. Usage reports	N	Admin can see some of this data, but it is not enabled to be viewed by users through their own application
Lockout notification	Y	
Online monitoring capability		
View audit log	N	The supply chain coordinator's admin only – not readily available to individual users
Parameter driven reports	N	The supply chain coordinator's admin only – not readily available to individual users

In comparing this chart to the one in the last section outlining option 1, there are many more "Yes" functions. These are in the areas of single sign-on, integration of affiliate sites, distributed user administration, and central policy management. What is not

supported in this approach are hierarchies, publishing privilege rights to other users outside of one's group, managing application specific data in the user profile, and advanced activity reporting made available to individual users.

Product Options

There are several companies who provide software and services centered around this approach. These companies include Netegrity, Securant, enCommerce (a division of Entrust), and Oblix. For the supply chain coordinator, GE recommends that Netegrity and Securant be evaluated for the portal management software solution. This is as a result of research conducted for GE Global Exchange Services deployments already in production and implementation experience in the General Electric Company.

There are several differences between the two products in architecture more than function. Netegrity is the market leader and has the most large scale implementations, including providing the base architecture for GE's global supplier portal and several other GXS solutions where the requirements were similar to the supply chain coordinator's. Securant waited longer to go to market, but by many accounts has a better future vision and more elegant architecture. Another significant different is that Netegrity is very focused on development around LDAP, where Securant uses database technology as the base under their directory structures.

In order to compare the two products, data is provided below from Giga Information Group. The following is a list of criteria used by Giga Information Group to evaluate web-based single sign-on products:

Multiple Authentication Types — All SSO products support passwords, of course. But some may support additional authentication types, such as biometrics, digital certificates, tokens or smart cards.

Authentication Method — The method differs from the type by representing the underlying authentication architecture. How well does the product handle the registration, suspension, etc.

Quality of Administration — In the case of employee SSO, the emphasis is placed on easy-to-use administrative console, intuitive commands and integration with user data repositories already in existence (e.g., human resources databases). Web SSO products are evaluated similarly, with the added point of distributed, subordinate administration — allowing multiple administrators to manage subsets of the user population.

Breadth of Supported Applications — How diverse are the supported target applications and platforms?

Granular Access Management — The Administrative console should permit the administrator to control authorization not only to certain applications, but also under certain conditions. Web SSO products are heavily weighed on this point.

Robust Architecture — How fault-tolerant and efficient is the underlying architecture of the product itself? How well does it scale to loads and to geographic distances?

Use of Directory Services — To what extent does the product rely on directories, compounded with the ability of that directory to be used for other purposes simultaneously?

End User Ease of Use — For employee SSO, this refers mainly to the familiar desktop experience and the elimination of normal log-in interruptions. For Web SSO users, this refers to the degree to which the user's desktop browser is modified in any way.

Vision — Also known as product road map, which vendor projects the most visionary use for its products during the next five years?

Costs and Timelines

For option 2 the assumption is that the security management solution software provides single sign-on, authentication management, entitlement management, distributed administration and affiliate services. Table 19 shows list of assumed functionality for the purpose of cost and level of effort estimation:

Table 19

Feature List	**Option 2: Netegrity or Securant Security Management Solution Software**
Distributed User Administration	Option 1 plus user registration service with the following directories technology: Netscape LDAP, NT Domains, Novell Directory Services, SQL Database, Oracle Internet Directory
Administrative Audit Trail	Basic User/Session/Application tracking
Access Management	Web interface to administer authorization and access control, secure portal management
Logon/Password Management	Basic authentication schemes, X.509, tokens, Forms, RADIUS, certificates and SSL
Reporting	Basic reporting from system/software logs
Policy Enforcement	Centralized basic policy-based management
Data Management	Basic access rules on data

Hardware

Once hardware is acquired, the supply chain coordinator may need to host the solution on a dedicated platform. This may require at least two standard server class machines, one for production and one for pre-production/backup. The supply chain coordinator may

choose to have a third box as a dedicated development and test environment or dedicated backup.

Product Training

For all developers who customize and build on the security platform, training may be required. The estimated time for training is a month per applied resource.

Resources

The following is an estimated list of resources that may be required to install and configure the security management solution software to provide the functionality in the table above.

- 1 project manager
- 1 system integrator
- 1 QA
- 1 security consultant

Estimated Project Length

Estimated project length is 2-3 months.

Option 3: Security Management Solution Software + Custom Administration

Option 3 addresses many of the delegated and self-administration requirements the supply chain community demands. While the product itself provide the ability to distribute administration features, most of these center around assigning access privileges for applications or resources. It does not take into account distributed administration of user specific data (preferences and data attributes) that may be required by the applications behind the supply chain portal. The basic product also does not capture and

consolidate events from multiple applications and make them available for viewing by individual users and group administrators.

Figure **80** is a flowchart of a process **8030** for a secure supply chain management framework. A plurality of users including suppliers, distributors, and stores of a supply chain are registered utilizing a network in operation **8032**. The registered users are maintained on a list in operation **8034**. Data from a plurality of stores of the supply chain is collected utilizing the network in operation **8036**. The list is updated to add, edit, and delete the users utilizing the network in operation **8038**. When a request (which includes an identifier) for access to the data is received utilizing the network in operation **8040**, the identifier is compared against the list in operation **8042** and a network-based interface is displayed in operation **8044** for allowing access to the data upon the successful comparison of the identifier against the list.

In one aspect, the identifier includes a password. In another aspect, the data is encrypted. In a further aspect, the list is updated upon receipt of a notice from at least one of the stores. In an additional aspect, only certain data is displayed based on the user being one of the suppliers, distributors, and stores. In one aspect, the network includes the Internet.

Setting Up a Unified Directory

Directory structure may be useful for extending the security management solution. The exact design of the directory may be the first task for an organization implementing the extended functionality for the supply chain coordinator. Directory design is beyond the scope of this engagement, but the following outlines the items to create directory structures that support the supply chain coordinator's needs.

1. Determine the Directory's Goals
2. Plan the Directory Data
3. Identify all data to go into the directory
    - Determined where the data may be mastered

- Determine who manages the data and who exactly may be allowed to update data
- Determine who can use the data and form
- Document the results

In identifying data, the question of what should go into the directory should be asked. The answer is data that is read often and written little:

- Data that can be expressed in simple object-attribute-value form
- Data useful for more than one audience
- Data accessed from more than one physical location

It is also important to ask what should not go into the directory. The answer is data that changes frequently, Large and unstructured chunks of data designed for file systems, ftp servers, web servers, or relational databases, data that requires sophisticated database operations to be accessed and manipulated.

4. Plan the Directory Schema
   - Identify all attributes needed to support a directory
   - Identify which attributes should be indexed
   - Identify all object classes needed to support a directory data
   - Determine if and how you may extend the schema
   - Document

The questions in planning the schema are how may the data be represented?

- What is the authoritative source of each data element
- Who is the owner for each element in the schema
- How is the data element updated in the directory and how often
- How often is the data accessed and in what way
- Would indexing the data element be productive for speeding up lookups?

5. Plan the Directory Tree
6. Plan the Security Policies
7. Plan for Replication and Referrals
8. Create the Implementation Plan

Extending the Directory to Meet Application Specific Requirements

Adding User Specific Attributes

Portal management solutions based on a directory include the ability to create extended attribute columns in the schema. Extended attributes can serve a number of uses by applications. Two common examples are user preferences such as language and local time. Once the directory structure designed by the process above is in place, the supply chain coordinator may need an application to allow users to manage their preferences and other data to be used by applications.

Figure **81** shows a schematic with attribute setting through a web interface **8100**. The figure shows an attribute **8102** that can be set through a web interface **8100**. The preferences are saved in the directory attributed **8104** to company_id and user_id **8106** (which together form a unique user in the system). Another example of attribute data pertaining to the supply chain applications could be to store single or multiple retailers a specific user can access data for.

For each attribute category the supply chain coordinator decides to include in the directory store, administration screens may be required to add, modify, or delete the attribute data.

Advanced User Privileges for Extended Directory Use

Once the application functionality specified previously exists, a new community management challenge presents itself. The question of who can access the new administrative features and what attributes they can update must be answered.

What makes this challenge much greater than managing privileges in Option 2 is that with the base configuration, privilege models are more simplistic and for the most part reserved for administrator users. Now that application-critical attribute data is being maintained by users themselves in a more distributed model, it may be helpful to make sure that the privileges to access applications and data are distributed properly.

At creation time, a user can get the following privileges:

Default privileges (defined by group type, user type and creator privileges, they are the intersection of these three sets of privileges, what is common to all of them).

Allowable privileges (creator privileges) These privileges are those, which the creator has, but are not included in the users default privileges.

Default privileges are assigned to the user at creation time (a trigger should be automatically fired), the *allowable* privileges may be granted if the creator choose to. The user privileges can be modified later by a user with sufficient privileges. That modifier user can revoke any privilege, (no matter if he/she has or does not have that privilege) and can grant only the privileges he/she has.

The administrative interface needs to be extended to allow for the addition of allowable features. The process by which default privileges may be assigned also needs to be customized in this approach. Once the more sophisticated privileges are in place, the update preference process is enhanced to check for proper access level. Figure **82** illustrates a flow diagram **8200** for assigning default privileges.

Once this information is stored and updated in the user profile **8202**, the application needs to update the current session. This requires that the session object be able to handle the attribute information so that it can be passed to applications that need it later (another piece of work).

Finally, though outside of the scope of the portal management solution, the applications that may use the extended attribute information must be programmed to correctly receive the information and put in into its application session.

Custom Privilege Templates

Another way to extend the security management solution to make administration easier is privilege templates. There should be privilege templates for each domain in the system. These focus on applications a certain type of user can access. For example, certain functions are only for the supply chain ember users. If there are certain things a user type can perform, making the administrator setup these privileges over and over again for each new user is a waste of time. Setting up a template for all users of that domain makes more sense. The domain privilege templates are created and maintained (add / delete privilege) by admin users.

Throughout the community there are many users who share a similar job function. Some of these differ within a domain, but some also are the same throughout the system. For example, every group may have an administrator regardless of domain. In order to save time in user setup, a user should be able to be assigned a role type that carries a certain number of privileges with it. The role may be used as a template to setup users, or the role might actually become an entity that privileges are assigned to, and whereby a user inherits those privileges by being attached to the role. Some roles may be setup for use across the system by the system administrator; the domain where the role is used may bound these. Other roles might be setup in a domain or group, depending on how much flexibility the supply chain coordinator decides to include in the solution.

The final piece to what a new user can be granted deals with the fact that a user can add only privileges that he/she was granted with, however he/she can delete any privilege that the grantee template contains.

Figure **83** shows a Venn diagram **8300** illustrating the intersection of privileges, i.e. domain **8302**, group **8304**, and granted **8306,** for a new user.

There should be a user interface for maintaining the tables where domain and role templates are stored. After a new domain or role is created in the system, a UI page is needed that allows the creator to attach newly created templates of privileges to the new domain or role. The creator can grant only his/her privileges.

Combined Activity Logging and Reporting

Another feature the supply chain community asked for was a single place to view the activities their employees perform in supply chain applications. In option 1, this was not possible, as there was not a single view of a user across applications. In option 2, there was single sign-on and the infrastructure to capture some user information across applications, but very little customization performed to take advantage of the infrastructure.

In option 3, two important functions are added. First, development is performed to increase the number of events that are captured about the user. This includes integration to the third party ASP applications to retrieve a set of user initiated events. These events are either stored in the security solution logs or in the supply chain coordinator's database.

The second part of this development effort includes building online visibility to the events captured for a group's administrator. This function gives the distributed community administrators the tracking capabilities they have asked for. These online views and reports should allow a group admin to see activities, both application access

related and perhaps even user actions within an application (depending on what the third party ASP applications can provide). There was also discussion during the workout sessions that the system might provide visibility for users within a company, with possible views including all registered users from their company.

Comparison to Requested Functions

In a previous section, the features requested by the supply chain community were detailed along with the functions those features imply. Table 20 shows whether functions are provided by this approach along with an explanation.

Table 20

Feature	**Y/N**	**Explanation**
SECURITY		
Lockout user after n unsuccessful logon attempts	Y	Supported
Notify administrator of lockouts	Y	Supported
On line monitoring		
Provide alternate passwords for lost/forgotten password situations		
Password expiration; require periodic password changes	Y	Supported
Acceptable password length parameters	Y	Supported
Ability to assign/select password	Y	Supported (not self-registration)
Ability to transfer logon intelligence.	Y	Agent to integrate affiliate sites.
Record all activities to the audit log	Y	Supported

Feature	Y/N	Explanation
COMMUNITY MANAGEMENT		
Distributed community administration	Y	Basic in this option.
Ability to add, change and delete users.	Y	Supported
Ability to assign access to users	Y	Supported
Ability to create roles or level of users	Y	Supported
Ability to set up default levels of access	Y	Supported
Ability to clone and/or access rights	Y	Supported with configuration
Mass delete of users		
Ability to copy a user ID		
Ability to export user load information from member backend.	N	Supported, but not implemented
User can be associated with multiple groups.	N	Groups here refers to organizations, which required customization
HIERARCHIES		
Ability to publish rights and privileges across hierarchies.	N	No hierarchies
Ability to authorize multiple levels of a hierarchy	N	No hierarchies
Ability to manage access against hierarchies	N	No hierarchies
Flexible data access and management.	Y	Custom extensions to support application specific data needed to

Feature	Y/N	Explanation
		control data access
DATA PUBLICATION		
User can view or access data in another sub-domain in their domain.	N	Not supported
User can view or access data in different domain.	N	Not supported
POLICY ENFORCEMENT		
Single sign on	Y	Supported
Ability to integrate with affiliates (i.e. other 3rd applications that make up the portal).	Y	Supported
Ability to interface with other applications: the supply chain coordinator 3rd party Remote hosts Platform independent	Y	Supported
Centralized policy management	Y	Supported
REPORTING		
The following community management reports were identified: Master user list Click and view access list User with published data authorization (i.e. users in other domains or sub-domains. Usage reports	Y	Custom

Feature	Y/N	Explanation
Lockout notification	Y	
Online monitoring capability		
View audit log	Y	Custom
Parameter driven reports	Y	Custom

From the comparison chart, this is a pretty comprehensive alternative. Still missing are the most complex community management items such as hierarchies and data publication across domains, but most other items are supported by this alternative.

Costs and Timelines

For option 3, the assumption is that the security management solution software provides more advanced administration features, self-administration, improved session tracking and event capture, detailed reporting, and custom policy extensions. Table 21 shows a list of assumed functionality for the purpose of cost and level of effort estimation.

Table 21

Feature List	Option 3: Security Management Solution Software + Custom Administration
Distributed User Administration	Option 2 plus, Custom approve/reject registration, grant/deny access to applications, grant privilege, modify user profiles, reports
Administrative Audit Trail	Custom User/Session/Application tracking
Access Management	Web interface to administer authorization and access control, secure portal management and custom agents.
Logon/Password	Basic authentication schemes, X.509, tokens, Forms, RADIUS,

Management	certificates and SSL. Custom notification and online monitoring
Reporting	Custom reporting integrated with monitoring systems
Policy Enforcement	Custom extension of the policy
Data Management	Custom extension

Software and Hardware

From a cost standpoint, Option 3 assumes that Option 2 has been implemented. Therefore, additional software license fees are not required. Additional hardware is probably not required, unless the load on the directory requires a separate installation of the supply chain coordinator decides to implement a reverse proxy server.

Resources

The following is an estimated list of resources that may be required to install and configure the security management solution software, develop custom administration, and develop custom reports to provide the functionality in the foregoing table.

1 project manager
1 business analysis
1 system integrator
2 web/database developers
1 QA, security consultant

Estimated Project Length

The estimated project length is 4-6 months (Dependent on completion of option 2)

Option 4: Adding Advanced Community Structures

The supply chain coordinator has a very unique community with real-world issues that defy standard organizational definitions. No two organizational structures or ownership

arrangements are the same. Yet being able to map the real world may be useful for fully meeting the community's requirements without clumsy workarounds.

The following section describes several custom additions that could be developed to push out community management to end-users and allow them to manage their web-based applications in a way matching their real-world business organization. Also presented is a way to dynamically manage the relationships between supplier, distributors, and retailers in place of a cross-reference method that requires constant update for application data access.

Each of the following would be custom developed application. While they would integrate heavily with the portal management solution and directory structure in options 2 and 3, they would be stand alone applications that would run in their own environment.

Creation of Hierarchies for Application and Data Access Control

Hierarchies are a way of representing real-world structures inside of an application. The purpose is to provide a more flexible way to manage the relationships between entities and other entities, entities and users, and users and data. Hierarchies are very complex to implement, especially in a many to many community such as the supply chain coordinator has. If implemented properly, however, they can provide group owners a way to manage their application and data controls that matches the way they see their own businesses and maps how they control functions in real life. This section attempts to lay out how hierarchies are implemented, maintained, and how they can be used to enhance privilege storage.

Creating and Managing Domains

The first step in creating a hierarchy is to create domains. Domains are the different types of groups that may exist in the portal, with each one requiring different business

rules for privilege assignment. An application function is needed to add a domain or remove a domain as shown below.

Figure **84** illustrates a diagram **8400** showing a system **8402**, supply chain member **8404**, retail manager **8406**, the supply chain coordinator **8408**, supplier **8410**, and distributor root nodes **8412**.

Creating and Managing Groups (Corporate Organizations)

Once domains exist, the next step is to setup groups within a domain. An example is the supplier domain. There are many different supplier companies, and each of these may have their own group (to control data access rights) even though they all share common application access rights. To technically describe groups under the top level domain, the term node is used. Nodes can be single level in nature or built in n-tiered structures, with each node having a parent node. In the case of a top level group, the parent node is the domain itself. An application function to add/modify/delete child nodes is required to add groups as shown in the diagram below.

Figure **85** illustrates another diagram **8500** showing groups **8504** within domains **8502**.

Groups exist within a domain. Therefore no matter what roles are created within a group, they are bounded by the privileges granted to a domain.

Adding Users to a sub-group (node) versus to companies

In a directory based security model (LDAP or NT), users typically belong to companies (groups). In the move to n-tiered hierarchies, there is also a move from the directory used by the SSO product to a relational database. This is because referential integrity is required to take full advantage of and properly manage hierarchies. By only allowing top level groups (not allowing an n-tired hierarchy), the hierarchies are easily synched to the

companies in the directory. If the supply chain coordinator chooses to enable sub-groups, however, users belong to nodes and not companies, and the path to the top node of each hierarchy instance identifies the corresponding company in LDAP. An n-tier hierarchy is shown below.

Figure **86** shows still another diagram **8600** showing hierarchies **8602**, in accordance with one embodiment of the present invention.

If n-tiered hierarchies are enabled, the management feature must also allow for nodes to be moved from one parent to another, as well as the ability to take a node and all nodes attached below it and move them together. Figure **87** shows a process **8700** for hierarchy management, in accordance with one embodiment of the present invention.

Figure **87** shows that this is an involved process requiring proper design, custom implementation, and testing.

Hierarchy Linkages for Data Access Control

In the initial stages, all information distributed by the supply chain coordinator to suppliers and distributors may be packaged by the supply chain coordinator. For example, in the pilot, the supply chain coordinator maintains a list of stores served by a specific distributor. When a report runs, it runs for all retailers associated in the cross-reference table to that distributor. To make sure information is correct, those cross-reference tables must be up to date. This approach also means that the supply chain coordinator is in control of what data can be viewed by a distributor, and there are very few controls over who within a distributor organization can view retailer information. The supply chain member has very little control over their data in this scenario, and the supply chain coordinator has a very high management overhead in this data exchange.

To perform more complex data access control, the supply chain coordinator may choose to implement linkages between organizational hierarchies. As described below,

hierarchies can be added to each domain (The supply chain coordinator, supplier, distributor, supply chain member, retail manager) to add application access flexibility. For data purposes, there can be links between nodes of one hierarchy and another. The most common usage of this would be a distribution center to a store.

Example: Looking at a large supply chain member and a distributor that serves them. A generic structure is shown in Table 22.

Table 22

supply chain member	Distributor
Corporate Group	Operating Group
Division	Region
State	Distribution Center
City / Area	Retailers
Retailer	

Figure **88** depicts a hierarchy **8800** in the supply chain portal management, in accordance with one embodiment of the present invention. In the supply chain members hierarchy, all retailers **8802** are attached to a level of node representing metropolitan areas **8804**. From the diagram before, each retailer of a supply chain member is associated with one (and only one) distribution center of a distributor. This allows a supply chain member to allow access for a distributor to access information for all retailers that they serve. But rather than assigning access for each retailer on its own (maintaining a cross-reference), the can leave the access control to the linkages created. This assumes that the linkages are maintained properly, but the advantage is that distributor access could be restricted to a level below the top level node without the need to update the access privilege every time a retailer status changed. The next section describes how this is technically implemented.

Hierarchy linkages for Data Publication

Each point in a hierarchy is a "node". Each node has a number or value assigned to it. This NODE_ID is numeric, unique system-wide and would enable the supply chain coordinator hierarchy system to clearly and unambiguous define in the application any location in the supply chain member, supplier, distributor, or retail outlet manager hierarchy.

Figure **89** illustrates the retail manager **8900** as part of the supply chain coordinator hierarchy **8902**, in accordance with one embodiment of the present invention.

The node ids or attributes become important in privilege setup. For example, initially a user named "Joe" might be part of the group "Restaurants." In a normal association, Joe would be able to see all data that belongs to his group. The access to data could be restricted in option 2 or 3, but that would have to be handled by the applications or through extended attributes with the actual store numbers in the portal management solution. There was not a concept of inherited data access or restricted data access through the use of nodes.

Now, assume that Joe is really a field auditor in the west restaurant manager division. As the restaurant manager admin, you want to setup Joe so that he can only access data for the West region, and cannot see the other divisions data. In the database portion of the security management system, the company id (restaurant manager) in the company id is replaced with a group id. Because the group id is a sub-group of the top level restaurant manager node, it can be associated back to the company_id that is stored in the directory.

Because Joe now belongs to group 503 and not group 500, he can only see data for restaurants from his node in the hierarchy and downwards. Note Table 23.

Table 23

Group Id	User Id	User Type	Priv. Id	Grantor Id	Restricted Node Id
503	Joe	the supply chain member	View Order Data	500	

Another case might be that while Joe works in the West Region, he actually only audits restaurants in the Tempe Metropolitan area. The columns can be added to the privilege to include other information such as a node that further restricts data access. With the privilege below, Joe can now only view order data for restaurants below node 506, even though there are more restaurants under the scope of node 503. Note Table 24.

Table 24

Group Id	User Id	User Type	Priv. Id	Grantor Id	Restricted Node Id
503	Joe	supply chain member	View Order Data	500	506

The concept of extending columns in the privilege store becomes very important when on organization has a requirement to grant access to applications and data to users in another group or another domain.

Granting Privileges Across Groups

Introduction

The requirement to grant access from one group to a user in another group comes from the complex ownership arrangements that the supply chain members have.

The supply chain members are the owners of the data (retailer information). They can publish (grant) their privileges to users in other organizations. The design for this is that supply chain members publish data in their hierarchy by:

- Granting access to retailers that belongs to their group or to groups downward in their (supply chain member) hierarchy.

- Granting access to specific retailers (many retailer ids).

- Granting access to retailers within a state or a zip code.

Example:

The grantor that belongs to 345- supply chain member node publishes the privilege to view order data to user Joe belonging to 123 supply chain member node. What Joe can see, so far, are the retailers the granter can see in his hierarchy, "R1", "R2", "R3"and "R4".

The grantor can narrow down the publishing by specifying a node in his hierarchy, let us say node 456. At this point, the user can see data for "R1", "R3" and "R4".

A "state" or "zip code" can narrow more the publishing.

Figure **90** is a schematic showing the process **9000** by which cross-domain access rights are granted.

Table 25 shows an example of how the privilege would be written to the central policy management.

Table 25

Group Id	User Id	User Type	Priv. Id	Grantor Id	Restricted Node Id	Restaurant Id(s)	Attributes (state/zip)
123	Joe	supply chain member	View Order Data	345	456		

Just the node numbers are stored in the directory. When the user is authenticated and accessing applications that need a store list in order to properly enforce data access rules, the custom application written in this alternative must access the hierarchies in the database. From the database, the application translates the intersection of the node ids into a list of valid stores that the user may perform the granted functions. This retailer list is then returned as part of the header strong to the resource requested.

You could even make this more granular by adding attributes for state or zip code associated with the nodes (especially the lowest node, which is a retailer).

Publication Functionality

The following is a list of publication functionality from a supply chain member point of view.

Publish any privilege a user has (and my data span of control) to users that need to perform actions for my retailers.

Publish all my privileges a user have (and my data span of control) to users that need to perform actions for my retailers (mainly for equal partners).

Revoke user publication.

Figure **91** is a diagram **9100** that shows a process flow for an administrative function. A publication can not be modified, it has to be deleted and then publish again. As with other custom developed community management functionality, a management interface to for granting privileges is required.

Publication Business Rules

A supply chain member can grant access to retailers that belong to their group or to groups downward their hierarchy. A user can see only items at retailer level if he/she got "privilege" published " to him/her. The supply chain member nodes and retailer ids should not be mutually exclusive, as a node can be specified but a retailer may also be specified.

Retailer ids and attributes should be mutual exclusive, either one can be specified, but not both. This is because attributes are restrictive, so by default any store specified must also have that attribute as part of it.

Only the grantor can revoke data publication.

The supply chain member does not publish data to users that belong to supplier or distributor hierarchy.

Suppliers or distributors can see data based on the retailers linked to their hierarchy without the supply chain member specifically publishing data (assuming the application permission has been granted to the supplier/distributor domain by the supply chain coordinator). There is no need for a supplier/distributor to see another supplier/distributor hierarchy data.

The supply chain member can publish data to the supply chain member users.

The supply chain members publish data to another supply chain member user only if the user is not in the same hierarchy with the grantor or if the user is in another branch of the hierarchy than the grantor.

Historical Requirements for Retailer Linkage

A very complex customization of the directory attributes would be to bound all privileges by start and end dates. The reason behind this optional function is that retailers often change hands. It was expressed in the workout sessions that members may need to view historical data for a specific retailer (from both the supplier/distributor side as well as the supply chain member side) even if they not currently own or serve that retailer. There are also legal requirements that may require this ability. Table 26 illustrates an example of this privilege.

Table 26

Group Id	User Id	User Type	Priv. Id	Grantor Id	Restricted Node Id	Retailer Id(s)	Attributes (state/zip)	Start Date	End Date
123	Joe	Supply chain member	View Order Data	345	456			1-1-2000	1-1-2001

As the number of attributes that need to be used by the application or translated into other information such as retailer numbers increases, so does application load. There are significant impacts on application performance and ease of use, as well as maintainability of both the portal management solution and the applications.

Auto associate store information

Figure **92** is a flowchart of a process **9230** for updating information in a supply chain management framework. A plurality of stores of a supply chain are registered utilizing a network in operation **9232**. The registration includes receiving first identification information. Data is collected from a plurality of stores of the supply chain utilizing the network in operation **9234**. This data relates to the sale of goods by the stores and includes second identification information more recent than the first identification information. Access to the data is allowed utilizing a network-based interface in operation **9236** so that in operation **9238** the first identification information can be compared with the second identification information in order to allow for the updating of the registration of the stores based on the comparison in operation **9240**.

In an aspect, the updating includes updating the first identification information to include the second identification information. In another aspect, the updating includes updating a distributor assigned to the stores based on the comparison. In further aspect, the first information includes a store identification number. In one aspect, the registration is further updated based on the data. In an additional aspect, the network includes the Internet.

The supply chain coordinator receives a load of updated retailer information from the retailer manager. This information is currently batch loaded into the SQL database and updates are made to tables matching retailers to suppliers, distributors, and supply chain members.

A desire is for the supply chain coordinator to automate this maintenance in the portal management solution as well. This is straight forward if the supply chain coordinator continues to use straight cross-reference between retailers and suppliers/distributors as the same tables may probably be accessed by the applications to determine data access in the application. But if hierarchies are used, there may need to be a custom application written to apply the following business rules.

When a new retail outlet is added, the application should check to see if that retailer already exists. If it does not, a new retailer entity should be auto-added to the proper group/ the supply chain member node.

Each time new retailer information in the address field arrives, the application may compare the new information to the retailer address information to see if data has changed. If yes, the retailer information is updated.

If the retailer is moved from a group node (deleted or reassigned) and it is the last retailer attached to a group node, the group node and corresponding supply chain member should be auto-deactivated.

Each time new retailer information arrives, the retailer's group/supply chain member information should be compared with the group/supply chain member # the retailer is already associated to. If it is different, the retailer should be reassigned (re-linked) to the appropriate group/supply chain member node. The Auto-add/delete processes may run as appropriate.

One issue may be how to auto-associate a retailer to the proper place in a node. In the design phase, available data elements should be examined to see if it is possible. If not, then there should be an "unattached" node not visible to applications outside of the hierarchy management. When the supply chain coordinator adds a retailer to a supply chain member, that member could assign it to the proper hierarchy point through the distributed administration.

A second issue may be where to associate the new retailer to the distributor or supplier node. There may the ability to pull attributes from the information the supply chain coordinator puts in their database (distribution center number or supplier ship from location). If an attempt is made to auto-associate the new retailer to other domains beyond the supply chain member's, a check process may be required to make sure the auto-association is correct, otherwise unauthorized data access could occur.

Comparison to Requested Functions

In a previous section, the features requested by the supply chain coordinator's community were detailed along with the functions those features imply. Table 27 shows whether functions are provided by this approach along with an explanation.

Table 27

Feature	**Y/N**	**Explanation**
SECURITY		
Lockout user after n unsuccessful logon attempts	Y	Supported
Notify administrator of lockouts	Y	Supported
On line monitoring		
Provide alternate passwords for lost/forgotten password situations		
Password expiration; require periodic password changes	Y	Supported
Acceptable password length parameters	Y	Supported
Ability to assign/select password	Y	Supported (not self-registration)
Ability to transfer logon intelligence.	Y	Agent to integrate affiliate sites.
Record all activities to the audit log	Y	Supported
COMMUNITY MANAGEMENT		
Distributed community administration	Y	Basic in this option.

Feature	Y/N	Explanation
Ability to add, change and delete users.	Y	Supported
Ability to assign access to users	Y	Supported
Ability to create roles or level of users	Y	Supported
Ability to set up default levels of access	Y	Supported
Ability to clone and/or access rights	Y	Supported with configuration
Mass delete of users		
Ability to copy a user ID		
Ability to export user load information from member backend.	Y	Custom
User can be associated with multiple groups.	N	But goal is accomplished with publish privilege feature
HIERARCHIES		
Ability to publish rights and privileges across hierarchies.	Y	Custom hierarchies
Ability to authorize multiple levels of a hierarchy	Y	Custom hierarchies
Ability to manage access against hierarchies	Y	Custom hierarchies
Flexible data access and management.	Y	Custom extensions to support application specific data needed to control data access
DATA PUBLICATION		
User can view or access data in another group in their domain.	Y	Custom

Feature	Y/N	Explanation
User can view or access data in different domain.	Y	Publication supports this, though only real case is the supply chain coordinator board member, and the supply chain coordinator may handle by system admin having a custom feature to assign access privilege to users instead of publishing privilege across domains
POLICY ENFORCEMENT		
Single sign on	Y	Supported
Ability to integrate with affiliates (i.e. other 3rd applications that make up the portal).	Y	Supported
Ability to interface with other applications: the supply chain coordinator 3rd party Remote hosts Platform independent	Y	Supported
Centralized policy management	Y	Supported
REPORTING		
The following community management reports were identified: Master user list Click and view access list User with published data authorization (i.e. users in other domains or sub-domains.	Y	Custom

Feature	Y/N	Explanation
Usage reports		
Lockout notification	Y	
Online monitoring capability		
View audit log	Y	Custom
Parameter driven reports	Y	Custom

Option 4 is the comprehensive community management solution. It requires a lot of customization, a lot of which occurs outside of the SSO/Portal Management solution. It does, however, meet all the functions specified by the supply chain community CTQs.

Cost and Timelines

For option 4, the assumption is that the security management solution software provides hierarchies, hierarchy management, and other customizations detailed in this section. Table 28 is a list of assumed functionality for the purpose of cost and level of effort estimation:

Table 28

Feature List	Option 4: Security Management Solution Software + Custom Administration with Advanced Community Structure
Distributed User Administration	Option 3 plus Custom hierarchical community structure at group/role/user level, structure to structure relationship, grant privilege across group, advanced administration features
Administrative Audit Trail	Custom User/Session/Application tracking
Access Management	Web interface to administer authorization and access control, secure portal management and custom agents.
Logon/Password	Basic authentication schemes, X.509, tokens, Forms, RADIUS,

Management	certificates and SSL. Custom notification and online monitoring
Reporting	Custom advanced reporting integrated with monitoring systems
Policy Enforcement	Custom extension of the policy
Data Management	Custom extension

Software and Hardware

From a cost standpoint, Option 4 assumes that both option 2 and 3 are already implemented. Therefore, additional software license fees are not required for security management software. Additional hardware is probably required to support the heavy application and database requirements for hierarchies and their use.

The following is an estimated list of resources that may be required to install and configure the security management solution software, develop the custom community management applications, and program custom data structures to provide the functionality in the table above.

1 project manager
1 business analysis
1 system integrator
2 or 3 web/database developers
1 QA
1 security consultant

Estimated Project Length

The estimated project length is 6-8 months (assumes completion of options 2 and 3)

Network Considerations

The supply chain coordinator can host the web portal itself, co-locate the portal servers at an ISP offering co-location services, or completely outsource the portal management solution (network and servers) to a managed service provider.

Hosting a Secure Portal

From a network view, the following details best practice for configuration of network servers for the portal.

One major issue may be managing a mission-critical network environment where users can execute transactions. The choice of ASP providers must also be a consideration.

Managed Services

A third option is to outsource all port, router, network and platform management. This is called managed services. There is a difference between managing up to the platform (OS) and the actual portal management solution.

The options for managed services to the platform level are the same players. Again, Level 3 is the only large national player in the Miami market. They do not offer managed services on their own, but have a partner program to provide these services. The actual partner for the southern region would need to be confirmed, but it is probably the same company that provides this service in the mid-Atlantic region, named AiNET. A company like AiNET would not have knowledge of the portal management solution itself, but would manage everything else from a security view including attacks against the network and the machines.

The next level of managed service includes actually operating and configuring the portal management solution. Companies in this class have resources already trained in the portal management solution and can take ownership of delivering the software and operating it for a community. Each provider has a number of partners in this area; GE Global Exchange Services is one of these companies. GXS provides managed Netegrity solutions along with others. Securant has many system integrator partners, though it is hard to tell who specializes in hosting and operating their solutions.

Application Security

Many of the applications that may sit behind the portal may be developed and operated by other organizations. The following details some recommendations for applications built on the NT platform using Microsoft framework and for evaluating ASP provided applications' security.

Recommended Policies

- Objects must be cleared before they are reused
- Errors during clearing must be handled in a way that ensures objects are not reused without clearing
- Browser caching directives must be used for sensitive pages
- Use of temporary files must be threadsafe
- Temporary files must be removed when no longer required

Approaches

- Clear after use
- Clear before use
- Use finally to ensure that objects are cleared

Vulnerabilities

- Database connection is reused, revealing another user's data
- Object pool includes one user's page with another's user page
- Caching algorithm inappropriately matches a request with a response containing another user's data
- Code Quality

Recommended Policies

- All code must conform to a consistent style guideline
- All code must be documented
- Intentionally complex code must be justified
- "Easter eggs" shall not be included in the code

Approaches

- Use style guideline from www.microsoft.com
- Use tools to enforce style guidelines
- Use design reviews to catch problems early
- Use peer reviews to prevent hidden problems

Vulnerabilities

- The more flaws the more likely one is to be exploitable by an attacker
- Poor code quality can rise to the level of a security problem
- Concurrent Programming

Recommended Policies

- No thread of execution within the application should be able to substantially affect any other thread

Approaches

- Synchronize access to all shared resources, including files and the session
- Eliminate all class and instance variables, unless final
- SingleThreadModel is not recommended for performance reasons

Vulnerabilities

- Information in shared resources can be inadvertently
- Debugging is difficult as these problems can be difficult to reproduce
- Database Access

Recommended Policies

- Parameters used in database queries must not be able to modify the intended query
- Results from queries must match the expected results
- Reliance on database permissions must be minimized and explicitly identified in the implementation
- The username and password used to access the database must have the minimum amount of privilege required by the application

Approaches

- Single encapsulated library for accessing databases
- Prepared statements should be used instead of ordinary statements

Vulnerabilities

- Queries can be modified to reveal data or corrupt database
- Debugging and Testing

Recommended Policies

- Code that is not used must be eliminated
- System.output.println() must not be used

Approaches

- Use an assertions framework
- Keep testing code separate from production

Vulnerabilities

- High likelihood that this code may inadvertently get enabled
- Security Organization and Metrics
- Security Roles
- Chief Security Officer

Develop Policy, Awareness and Training

- Define and Continuously Revise Corporate Policy and Standards
- Lead Company Wide Awareness and Training Program

Continuous Security Risk Assessing and Monitoring

- Enhance Assessment Tools
- Develop Security Dashboards and Scorecards
- Facilitate Session i

Champion New Security Initiatives

- Resource Planning and Budgeting

Drive Business Specific Security Strategic Planning

- Align Security Strategy with Business Objectives (e-commerce)
- Resource Planning and Budgeting

Owner of Security Measurements

- Session i, Security Self-Assessment, Corporate and Business Specific Security Measurements

Champion Policy Adoption and Training

- Take Security to the Masses
- Security Manager

Lead and Own New Security Initiatives

- Select and Package Latest Technology for New Security Initiatives
- Coordinate with Businesses to Rollout Initiatives

Deliver Company-Wide Architecture and Processes

- Define Technical Security Infrastructure (Single Sign-On,
- Intrusion Detection, Digital Certificates, VPN, etc)

Provide Technical Consulting to Businesses

- Assist Business to Resolve Business Specific Security Issues
- Security Administrator(s)
- Multiple people (Finance, IT, or distributed)

Project Execution of Technology and Process

- Responsible for Implementation in Business Site

Administration and Operation of Daily IT Security Activities

- Perform IT Security Tasks, Monitor Outsourcing Vendors and Coordinate with 3rd Parties
- Security Review Structure

The new technological infrastructure and its associated electronic reporting and feedback systems equips retailer management with accurate, timely, and previously unavailable information from the Supply Chain on sales, marketing and other performance indicators allow Supply Chain management to fully engage in managing supply and distribution processes and channels toward identified and agreed strategic objectives provide franchisees and retailers with the Supply Chain information they need to operate efficiently and make effective management decisions minimally impacts the resources of Supply Chain management.

With Supply Chain management assuming full responsibility for managing the fundamentals of the Supply Chain system, Supply Chain participants are strategically positioned to focus on the six business priorities that have been identified: operational excellence, boosting sales growth, focusing resources, discovering the essence of the Brand, image transformation and revitalizing franchisee relations.

Supply Chain Management

Figure **93** is a flowchart of a process **9330** for managing a health and personal care products supply chain utilizing a network. Such health and personal care products include pharmaceuticals, cosmetics, opticals, health carpe products, etc. A network is utilized in operation **9332** to receive data from a plurality of health and personal care products outlets of a health and personal care products supply chain in which the data relates to the sale of health and personal care products by the health and personal care products outlets. An electronic order form is generated in operation **9334** based on the data for ordering health and personal care products from a health and personal care